FINGERTEC

Benutzerhandbuch

Inhalt

5-6 Einleitung

Erleben Sie fortschrittliche Zugang skontrolle

Willkommen bei Ingress

10 nützliche Funtionen von Ingress

7-16 Kapitel 1

Installation und Konfigurierung

Einstieg - Ingress Installation

- Systemvoraussetzungen
- Start der Ingress Installation

Starting the Ingress Installation
Installation vom MYSQL SERVER
Installierend Microsoft .NET Framework 4.0
Installation des OFIS Scannertreiber.
Fertigstellung des Ingress DB Installationspro gramms.

Starten von Ingress

Quick Setup-Assistent

17-29 Kapitel 2

Verwaltung von Terminal und Tür

Terminals

- Terminal manuell hinzufügen
- Hinzufügen eines der Terminals durch Auto Scan.
- Geräte Konfigurieren
- Deaktivieren und Löschen des Terminals

Türen

- Hinzufügen von standalone Terminals zu Tür.
- Hinzufügen von Ingressus zu Tür
- Hinzufügen von Türschlössern (Keylocks) zu der Tür
- Konfigurieren Sie die Einstellungen zu den Türen.
- Löschen Gerät/Türen
- Zugangsgruppe der Tür
- Türereignisse

Verbindund mit IP Kamera

Tür permanent Öffnen oder Schließen Zeitzone.

Tür permanent Öffnen Schließen Urlaub Zeitzone. *(nur für Ingressus)*

30-35 Kapitel 3

Einstellung der Zonen

Antipassback

Feueralarm

Interlocking (*Ineinandergreifend*)

Wächterfunktion

Vier-Augen-Prinzip

Löschen Zone/Gerät/Benutzer Gruppe/ Vier-Augen-Gruppe.

36-45 Kapitel 4

Nutzerverwaltung

Abteilung hinzufügen

Benutzer hinzufügen

- Die Benutzer von Geräten herunterladen.
- Um die Benutzer mit USB-Stick herunterzuladen.
- Manuelles Erstellen von Benutzern

Bearbeiten von Personaldaten der Benutzer

- Um Information des Benutzers manuell zu bearbeiten
- Um Personaldaten des Benutzers aus einem anderem System zu importieren.

Nutzer auf Gerät hochladen

- Hochladen der Benutzer TCP/IP oder RS485.
- Hochladen der Benutzer durch USB-Stick.

Benutzer entfernen

- Aktuelle Benutzer entfernen
- Entfernen von Terminal- Benutzern

Weitere Operation

- Um die Personaldaten des Benut zers zu exportieren
- Um die Benutzer durch Schlaglwörter zu suchen

46-50 Kapitel 5
Zugriffsebenen
Zugriffsebene nach Zeit
- Einstellung des Zeitraums
- Einrichtung der Zutritts-Gruppe

Zutrittsebenen in den Ferien
- Einrichtung der Ferienzeiteinstellung
- Erstellen Sie die Ferienliste, um sie den Urlaubszeiteinstellungen hinzuzufügen

Zutrittseben durch Verifizierungstyp

51-55 Kapitel 6
Überwachung
Überwachung von Tür oder Zone
- Fern-Einstellungen
- Überwachungseinstellungen

Echtzeit-Überwachung
Zutrittsprotokoll
Visuelle Karte
- Einfügen von visueller Karte und Türen
- Starten des Überwachungsvorgangs

56-91 Kapitel 7
Zeiterfassung
Einrichtung der Zeittafel
Wöchentliche Zeittafeln
- Taktungsregeln
- Bereichsregeln
- Generelle Regeln
- Rundungsregeln
- Pausenregeln
- Überstundenregeln

Tägliche Plantafel
- Taktungsregeln
- Auswahlregeln
- Generelle Regeln
- Rundungsregeln
- Pausenregeln
- Überstunden Regeln

Die flexible Zeitplan
- Zeitplanungsregeln
- Generelle Regeln
- Rundungsregeln
- Pausenregeln
- Überstundenregeln

Aufbau von Dienstplan-Gruppe
- Erstellen eines wöchentlichen Gruppendienst planes.
- Erstellen eines Gruppendienstplanes
- Weisen Sie die Benutzer em Gruppen Dienstplan zu.
- Spezielle Arbeitsregeln

Benutzer Dienstplan
- Abwesenheit und Bemerkungen
- Hinzufügen von Abwesenheitsarten
- Hinzufügen von Bemerkungen

Anwesenheitsliste
- Anzeigen und Bearbeiten
- Herunterladen von Daten von Geräten
- Erstellen von Anwesenheitsdaten
- Export Anwesenheitsliste

Datenprüfliste

92-94 Kapitel 8
Bericht
Berichten und deren Anwendung
Vorschau, Drucken oder speichern von Berichten

95-102 Kapitel 9

Ingress Einstellungen

Datenbankkonfiguration

Systemparameter-Einstellungen

Felddaten-Management

Unternehmensinformationen

Systembenutzer

- Benutzerrollen erstellen
- Um ein Login-Konto zu erstellen und die Rolle zuzuweisen.

Ereignis

- Benachrichtigungen per Alarm und E-Mail konfigurieren.
- Alarmsignale und Farbe konfigurieren.
- E-Mail-Benachrichtigungen konfigurieren

Netzwerk-Kamera-Integration

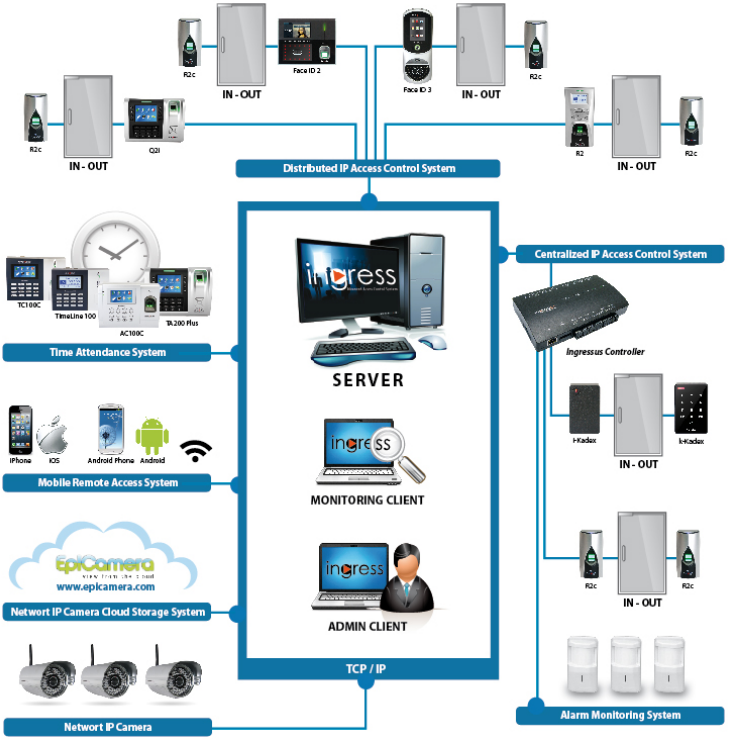
- Milestone-Server
- EpiCamera

Erleben Sie fortschrittliche Zugangskontrolle

Willkommen bei Ingress

Ingress ist eine fortschrittliche Zutrittskontrollsoftware, die als Komplettlösung entwickelt wurde. Mit Ingress können Sie die Fingertec Zutrittskontrollterminals und Ingressus Zutrittscontroller zentral verwalten und überwachen. Mit Ingress haben Sie die Möglichkeit, die oft umfangreiche und aufwendigen Konfiguration der Zutrittskontrolle zu zentralisieren, sowie sich alle Zutrittsereignisse zentral und in Echtzeit anzeigen zu lassen.

Ingress ist ideal für die Selbstverwaltung von Bereichen mit bis zu 100 Türen geeignet. Ingress bietet viele Zutrittskontrollfunktionen und die einfache Integration einer Alarmüberwachung oder diverser Einbruchmeldegeräte. Ingress unterstützt alle FingerTec Standalone Zutrittskontroll Terminals die mit Karte, Fingerabdruck oder Gesichtserkennung arbeiten. Verschiedene Terminals können über die Ingressus Netzwerksteuerung zusammengefasst und hierdurch mehrere Türen zentral überwacht werden.



10 nützliche Funtionen von Ingress

Effiziente zentrale Verwaltung
Ingress ist eine Server-client basierte Software, welche die Kontrolle von mehreren Computer gleichzeitig unterstützt. Sie beinhaltet nützliche Funktionen der Zugangsüberwachung, wie mehrstufige Benutzer und Benutzergruppen.

Sichere Architektur
Die Architektur von Ingress hält Daten sicher und zugänglich und bietet Ihnen in einer LAN-Umgebung Aktiviätenprotokolle, Datenzusammenfassung und moderne Gerätesuchfunktionen.

Benutzerfreundlich & Flexibel
Anwenderfreundlichkeit bedeutet bei Ingress Schnellinstallation, "drag-and-drop"-Methoden und hervorgehobene Verknüpfungssymbole mit Symlolleisten, um die Arbeit mit der Software zu vereinfachen

Verbesserte Software Sicherheitsmerkmale
Ingress bietet Ihnen die Möglichkeit eines Fingerabdruck Login für Systemadministratoren. Es gibt eine Bildschirmsperr- Funktion ebenso wie automatische Abmeldung nach Zeitüberschreitung. Die detaillierte historische Aufzeichnungen und Datenzusammenfassungs-Funktionen um früher Konfigurationsänderungen zu verfolgen Ingress verfügt auch über eine komplette Datensicherung und Wiederherstellung der Systemdaten.

Sofort verfügbare Zutrittskontrollberichte
Es stehen 13 verschiedene Berichtsarten zur Verfügung. Die Berichte unterstützen digitale Wasserzeichen, umfassende Ereignisfilterung, Schnelldruck und Email. Die Berichte können in 10 verschiedenen Formaten exportiert werden, u.a. xls, txt oder csv.

Nützliche Prioritäten und Alarmsignale
Sie können Alarmsignale organisieren und können Alarmprioritäten einstellen, um die Ansprechzeit von Ingress zu optimieren. Es gibt 62 Ereignistypen, die entsprechend der Notwendigkeit der Priorität zugeordnet werden können. Ingress wird automatisch eine E-mail-Benachrichtigungen zu zugeordneten Empfängern senden, wenn das System ein Ereignis feststellt. Sie können auch die Klangdatei für jede Priorität anpassen.

Leistungsstarke Zugriffseinstellungen
Ingress bietet eine Vielzahl von Zutrittskontrollfunktionen, wie Verriegelung, Feueralarmverknüpfung, Antipassback, Multi-Verifizierung und Mehrkartenbetrieb.

Integrated Monitoring
Ingress bietet Echtzeitalarm oder Ereignisprotokollierung, um sicher zustellen, dass alle Eriegnisse für das ganze System dokumentiert werden(einschließlich Nachrichten und Kontrollen). Türe können ferngesteuert werden, einschließlich Aufsperren der Türen und Unschafrschalten des Alarms.

Bildkarte für permanente Sichtbarkeit
Ingress kann eine Karte mit bis zu 9 Stockwerken für eine Echtzeitüberwachung zeigen. Die Bildkarte zeigt mit animierten Symbolen den aktuellen Status der Aktivität. Mehrere Arbeitsstationen können gleichzeitig überwacht werden.

Umfangreiche Zeiterfassungsfunktionen
Der Wochenplan besteht aus 3 Spalten "IN" / "OUT" für die Anwesenheitsüberwachung. Sie können Dienstpläne für Gruppen oder persönliche Dienstpläne vorbereiten, und sie Benutzern zuordnen. Ingress bietet auch Urlaub- und Ferienverwaltung. Im Anwesenheitsblatt, können Sie Daten einfach hinzufügen, bearbeiten, oder Anwesenheitsprotokolle löschen. Im Berichtsteil gibt es 6 Arten von häufig gebrauchten Anwesenheitsberichten, z.B.: tägliche Anwesenheit, Fehlzeiten oder Urlaubslisten.

Kapitel 1

Installation und Konfigurierung

In diesem Kapitel werden die Installation und Basiseinrichtung von der Ingress Software erläutert.

Bevor Sie Ingress nutzen können müssen Sie die Software ordnungsgemäß auf Ihrem Computer installieren. Die Installation von Ingress ist einfach. Das Ingress Installationsprogramm enthält einen Installationsassistenten, um Sie Schritt für Schritt bei der vollständigen Einrichtung der Software anzuleiten.

EINSTIEG - Ingress Installation

Systemvoraussetzungen

Bevor Sie Ingress installieren, stellen Sie bitte sicher, dass Ihre Client und Server PC auf dem neuesten Stand der folgenden Voraussetzungen sind:

Eigenschaft	*Server*
Betriebs-system	• Windows XP • Windows Vista • Windows 7, Windows 8 • Windows Server 2003/2008 • (32 oder 64 Bit)
Prozessor	Intel® Core® 2 Duo 2.5 GHz oder besser
Speicher	3 GB of RAM oder mehr
Festplattenlaufwerk	80 GB
Auflösung	1024 x 768 oder höher

Eigenschaft	*Client*
Betriebs-system	• Windows XP • Windows Vista • Windows 7 • Windows Server 2003/2008 • (32 oder 64 Bit)
Prozessor	Intel® Core® 2 Duo 2.0 GHz oder besser
Speicher	2 GB of RAM oder mehr
Festplattenlaufwerk	50 GB
Auflösung	1366 x 768

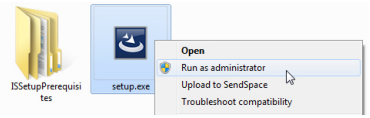
Installation des Systems

Damit Ingress ordnungsgemäß funktioniert, müssen Sie zunächst folgende Komponenten installieren.

- MySQL Server
- Microsoft .NET Sysetm 4.0 Voll
- FingerTec Ingress Software
- OFIS Scannertreiber

START DER INGRESS INSTALLATION

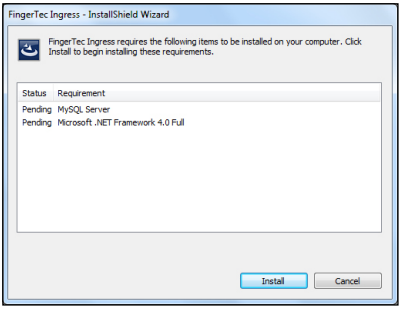
Rechtsklick auf die FingerTec Ingress Installationsdatei und wählen Sie [Als Administrator ausführen].



Sie werden nun aufgefordert Ingress Server- Installationsassistant zu starten. Der Installationsassistant zeigt die benötigten Komponenten des Installationsstatus. Es gibt 3 Komponenten, die installiert werden müssen, bevor wir mit Installation von Ingress beginnen können.

- MySQL Server
- Microsoft .NET Framework 4.0

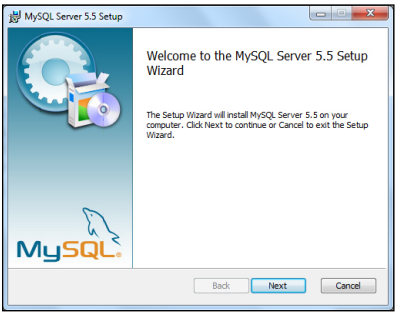
Klicke Sie auf Installieren um die Installation zu beginnen.

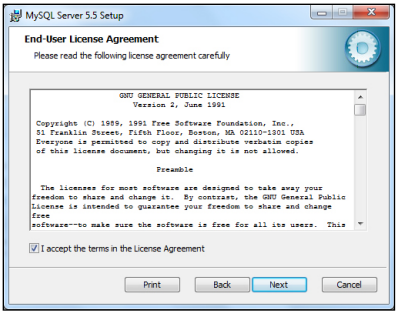

FingerTec Ingress - InstallShield Wizard
FingerTec Ingress requires the following items to be installed on your computer. Click Install to begin installing these requirements.
Status Requirement
Pending MySQL Server
Pending Microsoft .NET Framework 4.0 Full
Install
Cancel

INSTALLATION VOM MYSQL SERVER

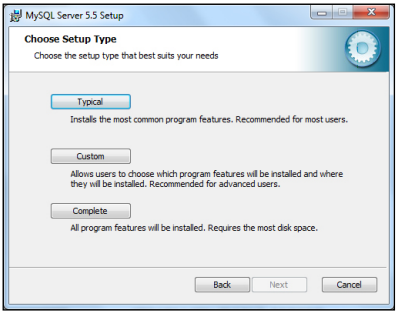
Der erste Bestandteil, der installiert werden soll,ist MySQL Server

Auf der Startseite, klicken Sie auf Nächste um fortzufahren. Am Ende des Lizenzvereinbarungfensters wählen Sie ich akzeptiere die Bedingungen der Linzenzvereinbarung aus und klicken Sie auf nächste, um fortzufahren.

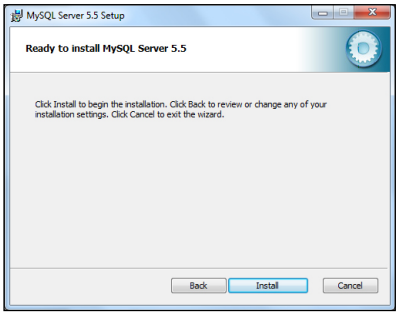

MySQL Server 5.5 Setup
Welcome to the MySQL Server 5.5 Setup Wizard
The Setup Wizard will install MySQL Server 5.5 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
MySQL
Back
Next
Cancel

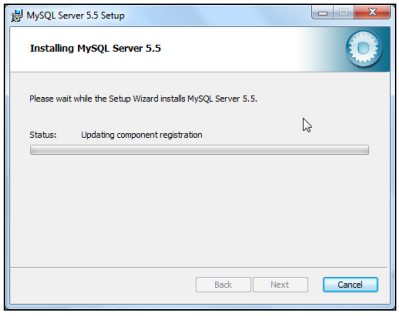

MySQL Server 5.5 Setup
End-User License Agreement
Please read the following license agreement carefully
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
I accept the terms in the License Agreement
Print
Back
Next
Cancel

Am Auswahl-Einstellungstyp Fenster, wählen Sie Typisch aus, um fortzusetzen.

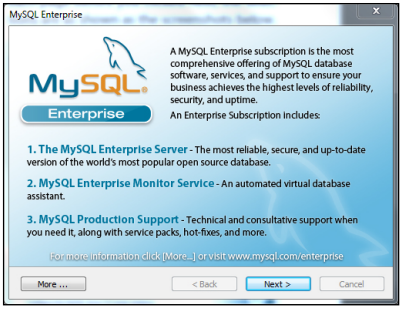

MySQL Server 5.5 Setup
Choose Setup Type
Choose the setup type that best suits your needs
Typical
Installs the most common program features. Recommended for most users.
Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.
Complete
All program features will be installed. Requires the most disk space.
Back
Next
Cancel

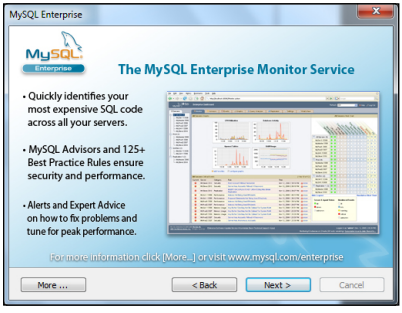
Auf bereit MySQL Server 5,5 Fenster zu installieren, klicken Sie Installieren, um sofort die Installation zu beginnen. Wenn die Fortschrittsleiste endet, wird das MySQL Unternehmen Fenster geöffnet.

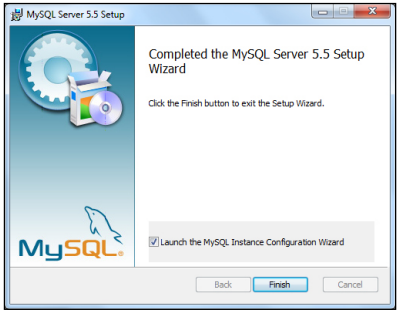

MySQL Server 5.5 Setup
Ready to install MySQL Server 5.5
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel



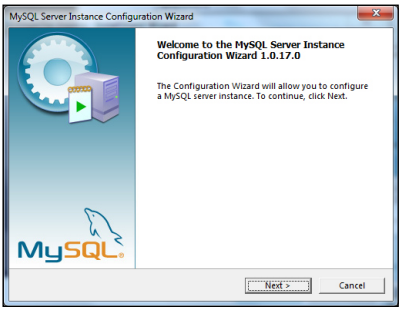
Am MySQL Enterprise-Fenster, klicken Sie auf Nächste > Nächste und Ende um MySQL Instanz-Server Konfigurationsassistent zu starten.

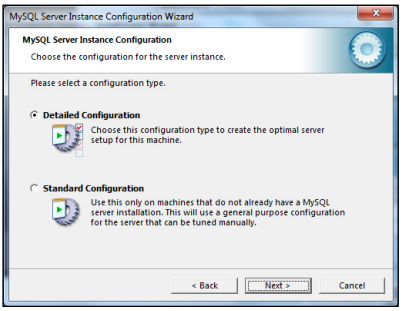

MySQL Enterprise
MySQL
Enterprise
A MySQL Enterprise subscription is the most comprehensive offering of MySQL database software, services, and support to ensure your business achieves the highest levels of reliability, security, and uptime.
An Enterprise Subscription includes:
1. The MySQL Enterprise Server - The most reliable, secure, and up-to-date version of the world's most popular open source database.
2. MySQL Enterprise Monitor Service - An automated virtual database assistant.
3. MySQL Production Support - Technical and consultative support when you need it, along with service packs, hot-fixes, and more.
For more information click [More...] or visit www.mysql.com/enterprise
More ...
< Back
Next >
Cancel

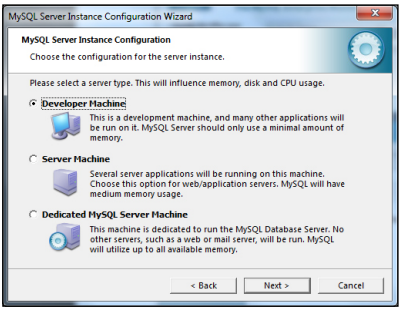

MySQL Enterprise
MySQL
Enterprise
The MySQL Enterprise Monitor Service
• Quickly identifies your most expensive SQL code across all your servers.
• MySQL Advisors and 125+ Best Practice Rules ensure security and performance.
• Alerts and Expert Advice on how to fix problems and tune for peak performance.
For more information click [More...] or visit www.mysql.com/enterprise
More ...
< Back
Next >
Cancel

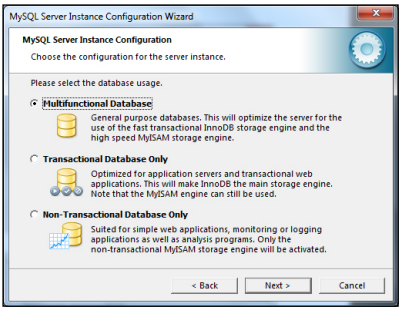


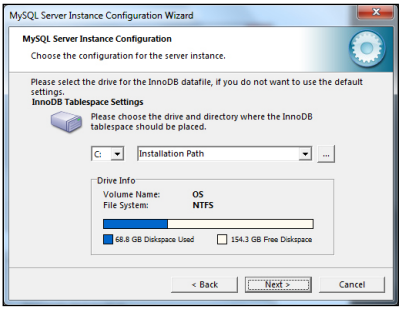
Sobald die Installation des MySQL Server endet, wird das Programm MySQL Server Instanz Konfigurationsassistent starten. Sie klicken 9 mal auf Nächste, bis Sie zum Sicherheitsoption erreichen. Stellen Sie sicher, dass auf jeder Seite, bevor Sie auf Weiter klicken, die Auswahl so darstellt ist, wie unten in den Bildschirmfotos.

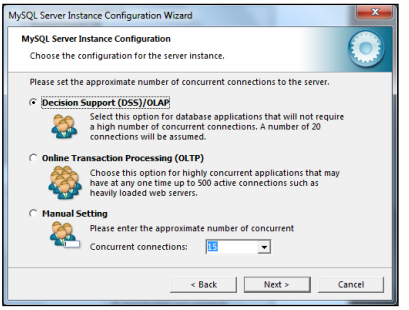

MySQL Server Instance Configuration Wizard
Welcome to the MySQL Server Instance Configuration Wizard 1.0.17.0
The Configuration Wizard will allow you to configure a MySQL server instance. To continue, click Next.
MySQL
Next >
Cancel

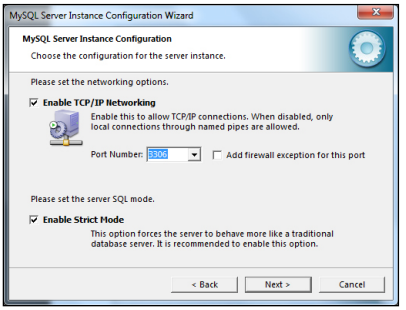

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Choose the configuration for the server instance.
Please select a configuration type.
Detailed Configuration
Choose this configuration type to create the optimal server setup for this machine.
Standard Configuration
Use this only on machines that do not already have a MySQL server installation. This will use a general purpose configuration for the server that can be tuned manually.
< Back
Next >
Cancel

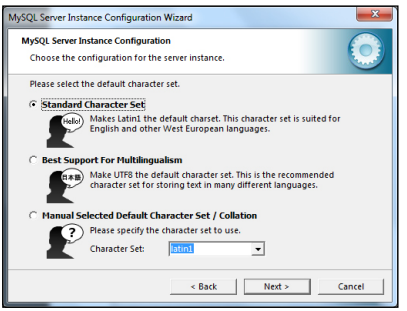

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Choose the configuration for the server instance.
Please select a server type. This will influence memory, disk and CPU usage.
Developer Machine
This is a development machine, and many other applications will be run on it. MySQL Server should only use a minimal amount of memory.
Server Machine
Several server applications will be running on this machine. Choose this option for web/application servers. MySQL will have medium memory usage.
Dedicated MySQL Server Machine
This machine is dedicated to run the MySQL Database Server. No other servers, such as a web or mail server, will be run. MySQL will utilize up to all available memory.
< Back
Next >
Cancel

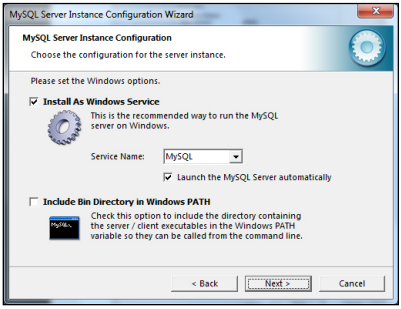

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Choose the configuration for the server instance.
Please select the database usage.
Multifunctional Database
General purpose databases. This will optimize the server for the use of the fast transactional InnoDB storage engine and the high speed MyISAM storage engine.
Transactional Database Only
Optimized for application servers and transactional web applications. This will make InnoDB the main storage engine. Note that the MyISAM engine can still be used.
Non-Transactional Database Only
Suited for simple web applications, monitoring or logging applications as well as analysis programs. Only the non-transactional MyISAM storage engine will be activated.
< Back
Next >
Cancel


MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Choose the configuration for the server instance.
Please select the drive for the InnoDB datafile, if you do not want to use the default settings.
InnoDB Tablespace Settings
Please choose the drive and directory where the InnoDB tablespace should be placed.
C:
Installation Path
...
Drive Info
Volume Name: OS
File System: NTFS
68.8 GB Diskspace Used
154.3 GB Free Diskspace
< Back
Next >
Cancel

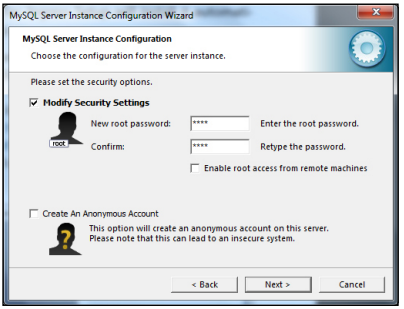

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Choose the configuration for the server instance.
Please set the approximate number of concurrent connections to the server.
Decision Support (DSS)/OLAP
Select this option for database applications that will not require a high number of concurrent connections. A number of 20 connections will be assumed.
Online Transaction Processing (OLTP)
Choose this option for highly concurrent applications that may have at any one time up to 500 active connections such as heavily loaded web servers.
Manual Setting
Please enter the approximate number of concurrent
Concurrent connections:
< Back
Next >
Cancel

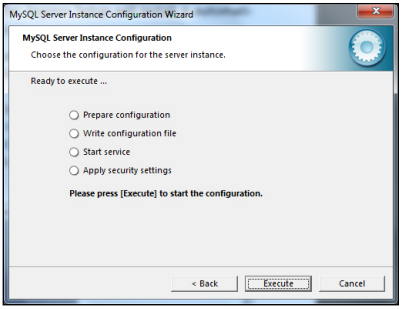

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Choose the configuration for the server instance.
Please set the networking options.
Enable TCP/IP Networking
Enable this to allow TCP/IP connections. When disabled, only local connections through named pipes are allowed.
Port Number: 3306
Add firewall exception for this port
Please set the server SQL mode.
Enable Strict Mode
This option forces the server to behave more like a traditional database server. It is recommended to enable this option.
< Back
Next >
Cancel

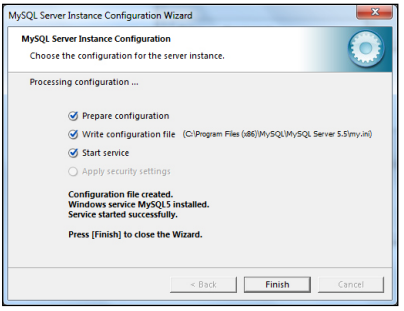

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Choose the configuration for the server instance.
Please select the default character set.
Standard Character Set
Makes Latin1 the default charset. This character set is suited for English and other West European languages.
Best Support For Multilingualism
Make UTF8 the default character set. This is the recommended character set for storing text in many different languages.
Manual Selected Default Character Set / Collation
Please specify the character set to use.
Character Set:
latin1
< Back
Next >
Cancel


MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Choose the configuration for the server instance.
Please set the Windows options.
Install As Windows Service
This is the recommended way to run the MySQL server on Windows.
Service Name:
MySQL
Launch the MySQL Server automatically
Include Bin Directory in Windows PATH
Check this option to include the directory containing the server / client executables in the Windows PATH variable so they can be called from the command line.
< Back
Next >
Cancel

Bei Sicherheitseinstellungen, geben Sie Ihren neues Root Passwort ein und bestätigen dies nochmal. Klicken Sie auf Weiter > Ausführen, um die Konfiguration zu starten. Danach, klicken Sie auf Ende.


MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Choose the configuration for the server instance.
Please set the security options.
Modify Security Settings
New root password:
Confirm:
Enter the root password.
Retype the password.
Enable root access from remote machines
Create An Anonymous Account
This option will create an anonymous account on this server. Please note that this can lead to an insecure system.
< Back
Next >
Cancel

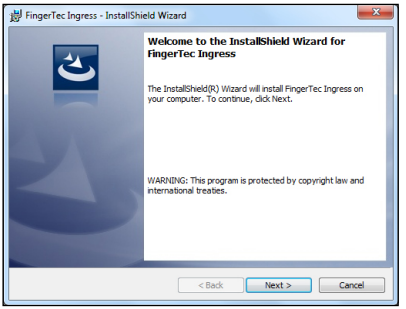


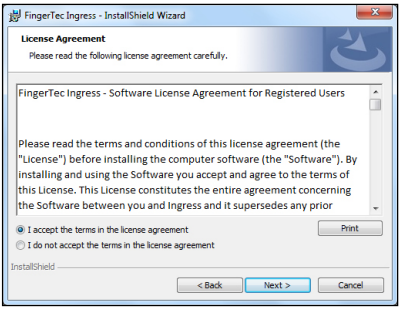


INSTALLIEREND MICROSOFT .NET FRAMEWORK 4.0

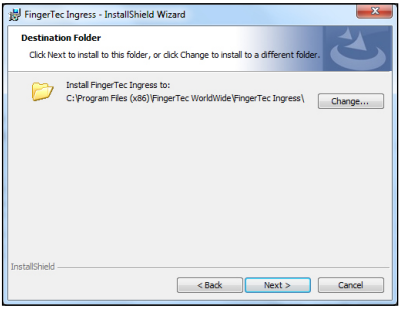
Die nächste Komponente, die das Intallationsprogramm fürdie Installation benötigt, ist Microsoft . NET Framework 4.0. Das FingerTec Ingress Setup wird feststellen und bestimmen, ob auf dem Computer bereit Microsoft .NET Framework 4.0 Installiert worden ist. Es wird die Installation überspringen, wenn es schon installiert worden ist. Wenn es nicht installiert worden ist, wird das FingerTec Ingress Setup es automatisch installieren.

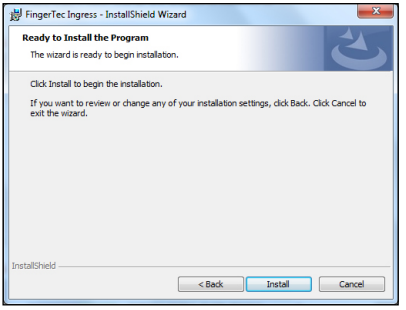
Nach Abschluss der Installation von MySQL Server und Microsoft . NET Framework 4.0 muss als nächste Komponente der Ingress Server installiert werden. Klicken Sie Weiter, wählen Sie ich akzeptiere die Bedingungen in der Lizenzverbindung und klicken Sie Weiter um fortzufahren. Wählen Sie den Installationpfad und klicken Sie auf Weiter.

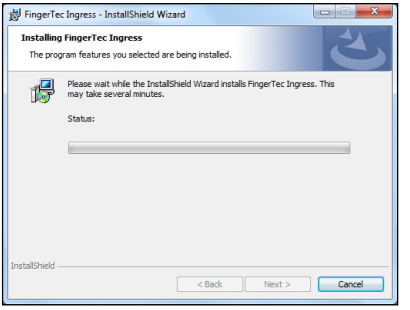

FingerTec Ingress - InstallShield Wizard
Welcome to the InstallShield Wizard for FingerTec Ingress
The InstallShield(R) Wizard will install FingerTec Ingress on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel


FingerTec Ingress - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
FingerTec Ingress - Software License Agreement for Registered Users
Please read the terms and conditions of this license agreement (the "License") before installing the computer software (the "Software"). By installing and using the Software you accept and agree to the terms of this License. This License constitutes the entire agreement concerning the Software between you and Ingress and it supersedes any prior
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

Wählen Sie Vollständig und klicken Sie Weiter. Klicken Sie auf Installieren, um die Installation zu beginnen und klicken Sie auf Fertig, wenn der Prozess abgeschlossen ist.


FingerTec Ingress - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install FingerTec Ingress to:
C:\Program Files (x86)\FingerTec WorldWide\FingerTec Ingress\
Change...
InstallShield
< Back
Next >
Cancel


FingerTec Ingress - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

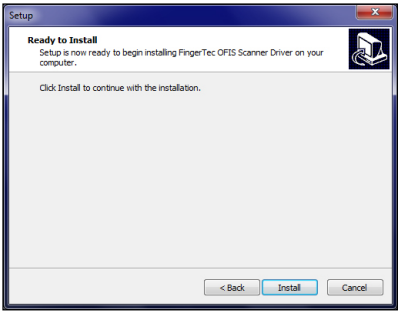

FingerTec Ingress - InstallShield Wizard
Installing FingerTec Ingress
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs FingerTec Ingress. This may take several minutes.
Status:
InstallShield
< Back
Next >
Cancel

ISTALLATION DES OFIS SCANNERTREIBER

Die letzte zu installierende Komponente ist der OFIS Scannertreiber. Das Ingress Setup wird feststellen und bestimmen, ob auf dem Computer bereits ein OFIS Scannertreiber Installiert worden ist. Es wird die Installation überspringen, wenn dieser schon installiert worden ist. Wenn er nicht installiert worden ist, wird das Ingress Setup ihn automatisch installieren.

Klicken Sie auf Weiter und klicken Sie auf Installieren, um die Installation zu beginnen. Nach dem Abschluss der Installation müssen Sie den Computer neu starten, damit die Änderungen wirksam werden. Bitte wählen Sie Nein, der Neustart wird auf einen späteren Zeitpunkt verschoben und klicken Sie auf Fertig, und fahren Sie mit dem nächsten Schritt fort.

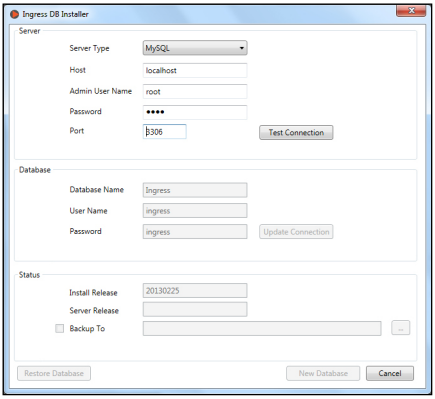
Setup
Welcome to the FingerTec OFIS Scanner Driver Setup Wizard
This will install FingerTec OFIS Scanner Driver 2.8 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel


Setup
Ready to Install
Setup is now ready to begin installing FingerTec OFIS Scanner Driver on your computer.
Click Install to continue with the installation.
< Back
Install
Cancel

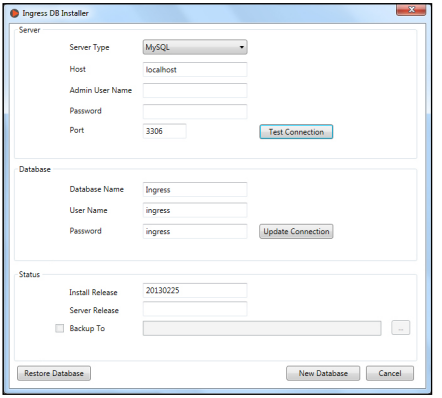
Setup
Completing the FingerTec OFIS Scanner Driver Setup Wizard
To complete the installation of FingerTec OFIS Scanner Driver, Setup must restart your computer. Would you like to restart now?
Yes, restart the computer now
No, I will restart the computer later
Finish

FERTIGSTELLUNG DES INGRESS DB INSTALLATIONSPROGRAMMS.

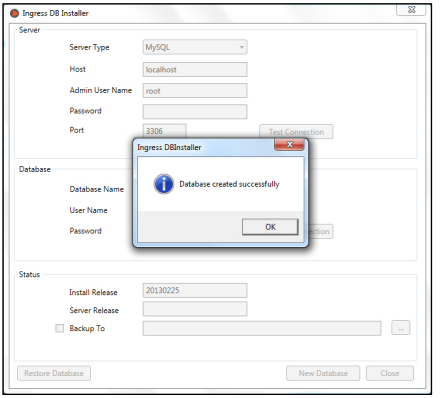
Das Ingress Setup wird nun das *Ingress DB Installationsprogramm Fenster öffnen. Es ist sehr wichtig, die Server- und Datenbankverbindung zu testen, bevor Sie Ingress starten.* Wenn Sie dieses Setup nicht ausführen, können Sie sich in Ingress nicht mehr einloggen.



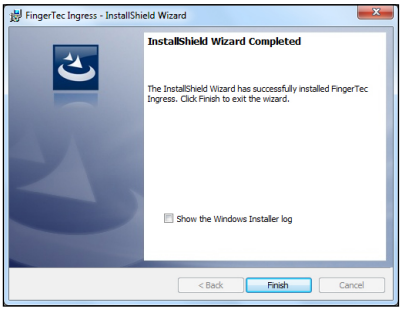
Wenn eine Verbindung zu dem Server erfolgreich hergestellt wurde, wird sich die Auswahl für die Datenbank öffnen. Geben Sie Benutzername und [Passwort] für die Datenbank ein und klicken Sie auf Aktualisieren.



Nachdem die Datenbankverbindung hergestellt wurde, klicken Sie auf Neu Datenbank, um die neue Datenbank zu erstellen.

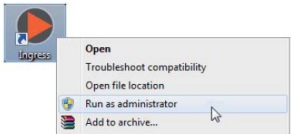


Klicken Sie auf Fertig, um Installationprogramm zu beenden.


FingerTec Ingress - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed FingerTec Ingress. Click Finish to exit the wizard.
Show the Windows Installer log
< Back
Finish
Cancel

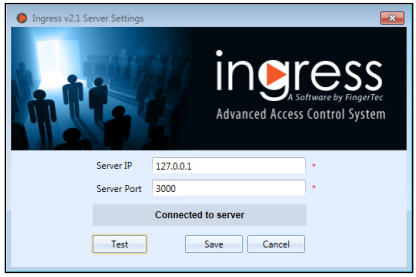
Starten von Ingress

Sobald die Installation beendet worden ist, wird das Ingress Symbol wird auf dem Desktop angezeigt. Klicken Sie mit der rechten Maustaste auf Symbol und wählen Sie Als Administrator ausführen.

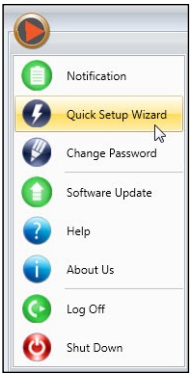


Der Ingress Client wird dir Datenbankverbindung aus dem Server validieren. Nach der Validierung geben Sie Server IP Adresse und Port ein, um die Verbindung herzustellen, klicken Sie auf Testen, um den Anschluss zu testen. Wenn die Verbindung erfolgreich hergestellt worden ist, klicken Sie auf speichern, um Server IP Adresse und Server Port im Computer für eine künftige Zugriff zu speichern.

Jetzt werden Sie zum Ingress Anmeldung Fenster kommen. Geben Sie bitte Benutzername und Passwort ein, um in Ingress einzuloggen. Standard - Benutzername: admin, Passwort: 123. Sie können den Benutzername und Passwort im Ingress Benutzerkonto ändern. Klicken Sie auf loggen, um in Ingress einzuloggen. Wenn Sie sich wünschen die Server Einstellungen zu rekonfigurieren, klicken Sie auf Server Einstellung. Statt mit Benutzernamen können Sie sich auch durch Fingerabdruck einloggen. Sie müssen Ihre Fingerabdruck Vorlage im Computer Benutzerkonto hinterlegen, bevor Sie sich durch diese Methode einloggen können.



Gratulation ! Sie sind bereit, Ingress zu erleben, die moderene Zugangskontrolle Software, präsentiert von FingerTec Worldwide.



Quick Setup-Assistent

Ingress wird den Quick Setup-Assistent beim der ersten Login-Sitzung starten. Das Programmassistent führt Sie durch alle Grundeinstellungen und nützlichen Einstellungen der Ingress Software.

Sie können den Assitent überspringen, um die Ingress Software selber zu konfigurieren. Sie können den Assistenten jederzeit aus dem Hauptmenü wieder starten.

Kapitel 2

Verwaltung von Terminal und Tür

Dieses Kapitel zeigt Ihnen, wie Sie die FingerTec Terminals in Ingress installieren, verwalten und den Türen zuweisen können.

Terminals

Terminals im Sinne dieser Anleitung sind die tatsächlich montierten Fingertec Terminals, um die Türen / Eingänge zu sichern.

- Es gibt 3 Arten von Terminals
- Ingressus Türkontroller
- Türschloss-Serie (Keylock 7700 und 8800)

Ingressus Türkontroller arbeiten zusammen mit dem abhängigen Terminal. Er ist das Modul, welches die Daten speichert und überträgt und die Türüberwachung und die Alaramaktivitäten verwaltet. Ingressus Türkontroller mit maximal 4 abhängigen Terminals verbunden werden (R2c, i-Kadex oder K-Kadex). Abhängige Terminals arbeiten nur als Datenerfassungsterminal für Fingerabdruck, Karte oder Passwort. Die erfassten Daten werden zu Ingressus für die Verfikation gesendet, bevor Ingress dem Benuter Zugang gewährt. Ingressus arbeitet mit AUX Eingabe (z.b.: Hitze und Rauchsensor, PIR Bewegungsmelder) und Ausgabe (z.b.: Alarmsirene, IP Kamera).

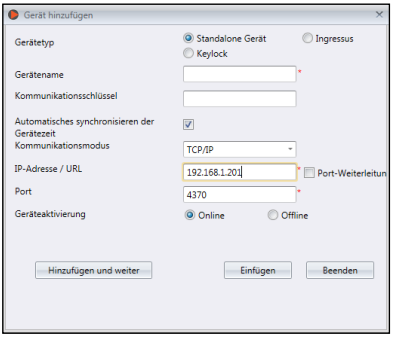
FingerTec standalone Terminals können mit allen anderen FingerTec Terminals verbunden werden, zum Beispiel R2, AC900, Q2i, Face ID Serie. Die Terminale haben individuelle Prozessoren und Speicher, die Benutzerdaten verfizieren und speichern. Standalone Terminals können mit abhängigen Terminals als ein Ein- und Ausgangssystem gepaart werden. Abhängige Terminals greifen Finderabdruck, Karte oder Passwortdaten ab und senden sie dann zum als Master installierten standalone Terminal zur Überprüfung.

Die Modelle der Türschloss-Serie bestehen aus Türbeschlag und mechanischem Türschloss. Die Modelle der Türschloss-Serie haben integrierte Prozessoren und Speicher die Benuterdaten verfizieren und speichern. Diese Modelle kommunizieren nicht direkt mit Ingress, sondern nur über einen USB Port für die Datenübertragung.

Terminal manuell hinzufügen

Sie müssen jedes Gerät in die Liste von Ingress hinzufügen, bevor Sie diese verwalten können.Das Hinzufügen von Geräten zu Ingress erfordert, dass das Gerät mit Ingress durch Netzwerk verbunden werden muss (TCP/IP oder RS 485). Darüber hinaus unterstützen die standalone Terminals und die Türschloss-Serie USB-Stick für Datenübertragung und Einstellungen mit Ingress. Jedes Gerät hat eine einmalige Seriennummer, die wichtig für Aktivierung in Ingress ist. Im Fall Sie die Online-Aktivierung nicht schaffen, kontaktieren Sie bitte Ihren lokalen Händler oder Vertriebspartner oder *support@fingertec.com* unter Angabe der Seriennummer des Gerätes.

1. Gehen Sie zu Gerät und wählen Gerät hinzufügen
2. Wählen Sie Gerätetyp und Übermittlungsmodus und dann fügen Sie dementsprechenden Informationen hinzu.



[Gerätename]: Benennen Sie das Gerät für ein leichteres zukünftiges Arbeiten.

[Kommunikation Passwort]: 5-stelliges Passwort zur Sicherung der Verbindung zwischen Gerät und Ingress. Ingress muss sich mit diesem Passwort mit dem Gerät (Unter DEV ID) paaren, bevor eine Verbindung hergestellt werden kann.

[Auto-synchronisieren Gerätezeit]: Aktivieren Sie diese Option, um Ingress zu erlauben, permanent das Gerät mit der Server-Uhrzeit zu synchronisieren.

Einstellungen der TCP/IP Verbindung:

IP Address/URL: Geben Sie die IP Adresse vom Gerät ein, so Ingress kann es im Netzwerk finden, um eine Verbindung herzustellen.

Für die Geräte, die an einem anderen Ort intalliert sind, können die URL des dortigen Servers in dieser Spalte eingeben. Ingress kann sich mit dieses Gerät durch das Internet verbinden.

Port: Standardmäßigen TCP Port (4370) des Ingress Servers mit Gerät durch Internet zu verknüpfen.

Einstellungen für RS485 Verbindung

Serieller Anschluss: Definieren Sie die serielle Schnittstelle des eingesetzten Server zum Verbinden zum RS232/485 Datenwandler.

Datenübertragungsgeschwindigkeit: Wählen Sie Baud-Rate des RS485 Netzwerkes

Einstellungen des USB-Sticks

Seriennummer: Seriennummer vom Gerät.

Geräte-ID: Stellen Sie sich sicher, dass Sie die gleiche ID eingeben, die im Gerät eingestellt wurde. Von 1 bis 999.

Einstellungen für Türschloss (Keylock-Serie)

Laufwerk und Pfad: Definieren Sie den USB-Stick, um die Basisinfromationen aus dem Türschloss zu lesen.

3. Klicken Sie das Kästchen online neben Gerät Aktivierung, um das Gerät in Ingress zu hinzufügen.

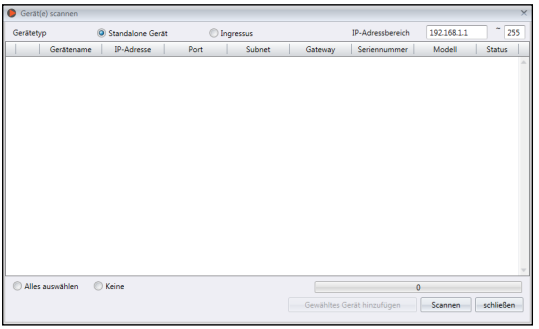
   Wenn eine Internetverbindung nicht verfügbar ist, können Sie das Gerät auch offline aktivieren. Ingress akzeptiert einen 12-stelligen Code für die Offline Aktivierung, den Sie bei Ihrem lokalen Händler oder über *support@fingertec.com* anfordern können.

4. Klicken Sie auf [Geräte Freigabe] , um eine Verbindung zum Gerät herzsutellen.

Bemerkung: *Sie müssen einen USB-Stick in Türschloss Keylock 7700/8800 stecken, um eine Dateiname "X_uduta" herunterzuladen, wobei X die Geräte ID des benutzen Geräts ist (z.b: 1_uduta). Die Datei enthält die Seriennummer vom Gerät und andere wichtige Information. Ingress kann Keylocks 7700/8800 in der Liste hinzufügen,nachdem diese Datei auf USB-Stick erfasst wurde.h disk.*

Hinzufügen eines der Terminals durch Auto Scan.

Falls Sie nicht die bestimmte IP Adresse des Einzelgerätes oder Ingress wissen, können Sie die Auto Scan Funktion verwenden, um sie im Netzwerk zu suchen.



1. Klick Sie Scan Gerät
2. Wählen Sie Gerätetyp

   Standalone Gerät: Bitte tragen Sie die IP Adresse ein.

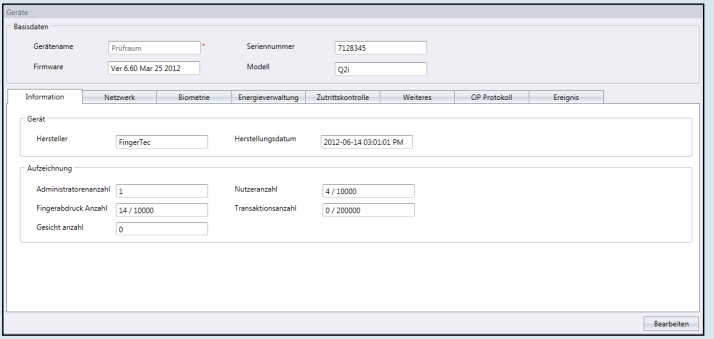
   Ingressus: Ignorieren Sie IP Adresse, weil Ingress die IP Adresse von Ingressus automatich finden kann.

   Keylock: Ingress scannt Ihr USB Laufwerk nach der "X-Udata" Datei.
3. Klicken Sie Scannen, um zu starten.
4. Das Gerät wird entdeckt und taucht in der Liste auf.
5. Wählen Sie die Geräte, um sie in Ingress zu hinzufügen.
6. Fahren Sie mit der Aktivierung des Gerätes fort *(Siehe Kapitel 2 . Geräte manuell hinzufügen)*.

Geräte Konfigurieren

Laden Sie alle Einstellungen und Information von den Geräten, nachdem die Verbinding hergestellt ist. Sie können die Einstellungen für jedes Gerät personalisieren und neue Einstellungen und Information zu den Geräten duch Hochladen synchronisieren. Aufgrund der unterschiedlichen Natur der 3 Gerätearten verbirgt Ingress einige Seiten / Optionen, wenn die für ein Gerät nicht anwendbar sind.

1. Klicken Sie auf Gerät auswählen.
2. Klicken Sie auf laden Sie die Geräteeinstellungen herunter.
3. Warten Sie, bis der Herunterladevorgang abgeschlossen ist.
4. Beginnen Sie, zu konfigurieren.



Information: Auf dieser Seite werden die ganzen Information zum Terminal dargestellt. Es sind keine Änderungen möglich. Sie können dort auch den Speicherstatus des Terminals erfahren.

Netzwerk: Sie können die Kommunikationsmodui auf dieser Seite ändern, zum Beispiel Änderungen von TCP/IP zu RS485. Sie können die Einstellungen TCP/IP aktualisieren (z.B: in neue IP Adresse ändern) oder RS485 Einstellungen (zB.: Baud-Rate zu 9600bps zu ändern). Alle neuen Einstellungen werden erst wirksam, nachdem Sie die neuen Einstellungen zum Gerät hochladen.

Biometrisch: Diese Seite benötigen Sie nur, wenn Sie eine Verbindung mit Terminals haben, die Fingerabdruck und Gesichtserkennung unterstützen. Ändern Sie dementsprechend die Einstellungen, nachdem Sie auf "Bearbeiten" anklicken.

1:1 Verifikation: Setzen Sie standardmäßig auf "NEIN", damit die Bunutzer den Zugang sofort nach der Überprüfung ihres Fingers oder ihres Gesichts erhalten können. Ändern Sie zu "Ja", wenn Sie wollen, dass die Benutzer ihre ID vor der Fingerabdrucküberprüfung oder der Gesichtsüberprüfung eingeben müssen.

Figerabdruck-Algorithmus: VX 10.0 ist der neueste Algorithmus für Fingerprinterkennung, der vom Gerät unterstützt wird. Ändern Sie nur auf VX 9.0, wenn Ihre Umgebung (angeschlossene Terminals) den alten Algorithmus benutzt. Diese Option gilt nicht für Ingressus, weil sie nur VX10.0 unterstützt .

Gesicht / Fingerabdruck 1:1 Zurückweisungsschwelle: Die ist das Niveau der passenden Sicherheit/Erkennungsgenauigkeit für die Option, dass die Benutzer die Benutzer-ID vor der Verifizierung des Fingerabdrucks / des Gesichts eingeben. Für den Fingerabdruck geht der Regelbereich von 0 bis 50, wobei 50 die höchste Sicherheit ist. Für das Gesicht beträgt der Regelbereich von 0 bis 99, wobei 99 die höchste Sicherheit ist. Die voreingestellten Standardwerte sind 15 für den Fingerabdruck und 70 für das Gesicht.

Gesicht / Fingerabdruck 1:N Zurückweisungsschwelle: Das Niveau der passenden Sicherheit wenn Sie die Benutzern Verifizierung mit Fingerabdruck/ Gesicht ohne Eingabe der Benutzer-ID erlauben. Die voreingestellten Standardwerte sind 45 für den Fingerabdruck und 75 für das Gesicht.

Power: YSie können die Dauer (in Minuten) konfigurieren, die das Terminal wartet, bevor es in den Standbymodus geht.

Wartezeit (in Minuten): Die Zeitdauer,die das Gerät wartet, bevor es in den Standbymodus geht.
Idle Action: Wählen Sie, was nach Ablauf der Wartezeit passiert, Ruhezustand oder Auschalten.
Die Einschaltzeit: Kreuzen Sie das Kästchen an und setzen Sie die Zeit ein, wann das Gerät einschalten soll.
Die Ausschaltzeit: Kreuzen Sie das Kästchen an und setzen Sie Zeit ein, wann das Gerät abschalten soll.

Zugangskontrolle: Sie können das Gerät für die Grundeinstellungen der Zugangskontrolle konfigurieren.

Speichern Sie das Transaktionsprotokoll: Speichern Sie das Transaktionsprotokoll: Setzen Sie standardmäßig auf JA. Das Gerät speichert IN-OUT Ereignisse der Benutzer. Falls Sie wollen,dass das Gerät nur die Zugänge ohne Speicherung kontrolliert, wählen Sie NEIN. Das Gerät wird dann keine IN - OUT Ereignisse speichern.

Speichern Sie Fehlversuche: Setzen Sie standardmäßig auf "JA". Das Gerät speichert auch die Zutrittsversuche, die fehlgeschlagen sind. Sie können so die Fehlversuche auswerten und ggf. die biometrischen Einstellungen ändern und anpassen, um den Prüfprozess zu verbessern. Wählen Sie NEIN aus und das Gerät wird dann keine Ereignisse speichern.

Master-Record-State: Sie müssen das Gerät als Master oder abhängiges Gerät (Slave) definieren, wenn zwei unabhängige Geräte intalliert wurden, um eine Tür zu kontrollieren. Normalerweise wird das unabhängige Gerät, das den Eintritt kontroliert,wird als Master eingesetzt, und am Ausgang ist das abhängiges Gerät. Ignorieren Sie, wenn Sie ein Slave-Gerät mit einem unabhängigen Gerät installieren. Das ist wichtig, wenn Sie eine Antipassback-Funktion benutzen. Das Master-Gerät speichert alle Eingangs-Ausgangs Rekorde, um den Antipassback-Status auszurichten.

Antipassback: Funktion, die die Benutzer zwingt, sich bei jedem Zu- oder Ausgang in oder aus einer Zone zu verfizieren. Sollte ein Benutzer durch dichtes Aufschließen zum Vordermann ohne Verifizierung Zugang in die Zone Zugang erhalten, wird das Gerät seine Verifizierung für zukünftige Zugänge sperren. Sie können eine der folgender Einstellungen auswählen, um Ihre Umgebung anzupassen.

Rein: Aktivieren Sie das, um den Benutzer beim Verlassen der Zone zur Verifizierung zu zwingen. Benutzer können die Verifizierung überspringen, wenn sie in der Zone hereinkommen.

Raus: Aktivieren Sie das, um den Benutzer beim Eintritt in die Zone zur Verifizierung zu zwingen. Benutzer können die Verifizierung überspringen, wenn sie die Zone verlassen.

Rein/Raus: Aktivieren Sie das, um die Benutzer bei Ein- und Austritt zur Verifizierung zu zwingen.

Nicht & Speichern: Wählen Sie diese Einstellungen, dass das Gerät die Benutzer nicht bei wirksamen Antipassback sperrt. Das Gerät wird nur die Übersicht über Antipassback Ereignisse der Benutzer-ID speichern, wobei Sie die Rekorde im Ingress herunterladen können, um sie anzuschauen und zu analysieren.

Keine: Deaktivieren Sie den Antipassback an dem Gerät.

andere Einstellungen

Das Gerät ausschalten: Um das Gerät durch Fernsteuerung auszuschalten. Kein Terminal hat eine Ausschalttaste, um unberechtiges Ausschalten zu verhindern. Sie können das Gerät herunterfahren/ausschalten, indem Sie auf diesem Taste anklicken.

Gerät Neustarten: Um das Gerät neuzustarten. Wenn das Gerät eine Fehlfunktion hat, starten Sie es neu.

Synchronisation von Datum und Uhrzeit: Synchronisieren Sie sofort das Datum und die Zeit vom Gerät. Es wird empfohlen, dies während der ersten Installation zu tun.

Herunterladen Sie Gerät Einstellungen: Zum Herunterladen von Einstellungen/Parametern vom Gerät.

Aktivieren Sie das Gerät: Aktivieren Sie das Gerät, um es Ingress zu hinzufügen.

Alle Daten des Gerätes entfernen: Die Speicherung des Gerätes löschen, um es auf Werkseinstellungen zurückzusetzen. Danach können Sie keine Daten abrufen.

Alle Protokoll löschen: Um alle Transaktionsprotokolle zu löschen, die im Gerät gespeichert werden. Es wird empfohlen dies erst zu tun, wenn Sie mit dem Herunterladen der Protokollen vom Gerät fertig sind.

Admin-Privileg löschen: Um die Administratoren-Sperre im Gerät zu löschen. Jeder Anwender kann dann das Hauptmenü durch Drücken der Taste MENU betreten. Machen Sie das nur, wenn Sie dem Gerät einen neuen Administrator zuweisen wollen.

Laden der Einstellungen des Gerätes : Um alle neue Einstellungen / Parameter des Gerätes hochzuladen.

Betriebsprotokolle: Das Gerät speichert jede Operation, die von den Adminitratoren in der Protokolldatei gemacht werden. Das ist eine versteckte Datei, die Sie nicht im Gerät sehen können. Sie müssen die Betriebsprotokolle in Ingress herunterladen, um die anzuschauen.

Drücken Sie [herunterladen OP] Taste, um vom Gerät herunterzuladen.

Bestimmen Sie den Datenumfang, um Ihre Suche einzuengen.

Ereignis: Das Gerät nimm ungewönliche Aktivitäten (z.b.: Tür Gewaltsam öffnen, Alarm, falsche Verifizierung, usw.) als Ereignisauf. Diese Daten werden automatisch in Ingress heruntergeladen. Sie können Ihre Suche weiter eingrenzen, um nach Datum und Uhrzeit zu schauen.

5. Klicken Sie auf Geräteeinstellungen hochladen,um neue Einstellungen auf das Gerät zu laden.

Deaktivieren und Löschen des Terminals

Löschen Sie oder entfernen Sie das Gerät aus der Liste, wenn es nicht mehr verwendet, oder irrigerweise zum Ingress hinzugefügt wurde. Falls Sie ein Gerät vom Ingress entfernen wollen (um die Datenübertragung mit dem Gerät zu stoppen), deaktivieren Sie es auf der Liste.

Ein Gerät zu löschen

1. Klicken Sie auf das zu löschende Gerät aus der Liste.
2. Klicken Sie auf Gerät zu löschen.
3. Klicken Sie auf Ja, um zu bestätigen, das Gerät zu löschen

Terminals deaktivieren:

1. Klicken Sie auf das Gerät aus der Liste, welches deaktiviert werden soll.
2. Klicken Sie auf Gerät zu deaktivieren.
3. Klicken Sie auf Ja zum Bestätigen der Deaktivierung des Gerätes.

Türen

Terminals werden zu Ingress hinzugefügt, um eine Liste der Geräte zu erstellen, die m Umfeld installiert wurden. Jetzt können Sie beginnen,die Geräte mit der Türen dementsprechend zu verkoppeln. Sie müssen die Geräte zuweisen, um jede Tür zu überwachen. Durch die Paarung mehrerer Geräte an eine bestimmte Tür, wird ermöglicht, die gleichen Zugriffseinstellungen (z.B. Entriegelungszeit) der Eingangsgeräte und der Ausgangsgeräte vorzunehmen.

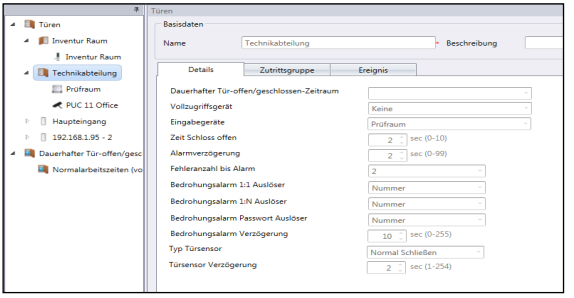
Durch Installation von Ingressus II (2-Türen-Tür-Kontoller), können Sie Geräte mit 2 Türen paaren.Sie können verschiedenen Zugangseinstellungen für jede Tür konfigurieren, obwohl sie mit dem gleichen Ingressus II Kontroller verbunden werden.

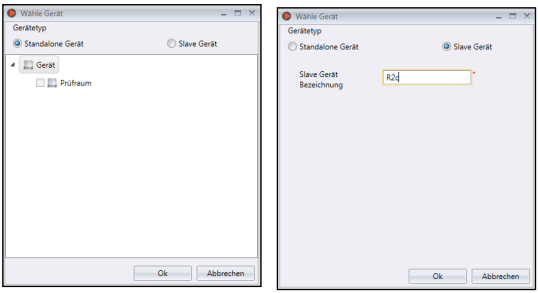
Arten vom Gerät	Anzahl der Geräte/abhägige Geräte	Anzahl der Türen
Standalone Geräte	2 Geräte	1
Ingressus I	2 Abhängige Anschlussgeräte	1
Ingressus II	4 Abhängige Anschlussgeräte	2
Türschloss (Keylock)	1	1

Ingress kann mit Video-Überwachungssoftware verbunden werden. Sie können diese zum Milestone Server oder EpiKamera verbinden, um Video von Ihrer IP Kamera in Live-Ansicht oder als gespeicherte Wiedergabe streamen. Es wird empfohlen, die IP Kamera mit dem Eingang zu verbinden, an dem das Gerät intalliert wurde, um die Bewegung der Benutzer zu überwachen. Im Fall von ungewöhnlichen Türkktivitäten (z.b.: Tür gewaltsam geöffnet, Gerät ohne Berechtigung entfernt) löst Ingress Alarmen aus, um die Administratoren zu warnen. Sie können das gespeicherte Video von diesem Zeitpunkt abspielen, um zu wissen, was an der Tür passiert ist oder sogar die Fotos oder Videos für weitere Untersuchung exportieren.

Hinzufügen von standalone Terminals zu Tür

1. klicken Sie Tür in der linken Leiste
2. Klicken Sie Tür hinzufügen.
3. Bennen die Tür um, zum Beispiel Haupteingang.
4. Schreiben Sie eine Beschreibung an der Tür für Ihre einfache Referenz.

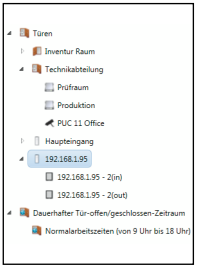




5. Klicken Sie auf Geräte hinzufügen.
6. wählen Sie Standalone Gerät.
7. Wählen Sie das Gerät um es dieser Tür zu hinzufügen.
8. Wiederholen Sie den Schritte (5) bis (7), um ein weiteres standalone Gerät zu dieser Tür hinzuzufügen.

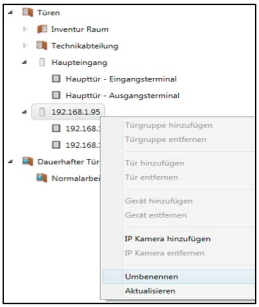
Bemerkung: *Wählen Sie [abhängiges Gerät] im [Gerät hinzufügen] Fenster, wenn Sie ein abhängiges Gerät (R2c, i-Kadex or K-Kadex) mit einem unabhängigen Gerät in Verbindung setzen. Nennen Sie das abhängige Gerät nach seinem Modell.*

Hinzufügen von Ingressus zu Tür

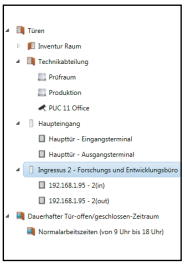


Ingress kreiert automatisch Tür(en) nachdem Sie Ingressus in das System hinzugefügt haben. Das System schafft 1 Tür, wenn Ingresses I als Gerät hinzufügt wird, 2 Türen, wenn Ingresses II hinzufügt wird. Sie sehen die IP Adresse von Ingresses in der linken Leiste.

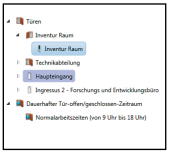
Bei Ingressus II werden Sie 2 Zeilen mit der gleichen IP Adresse senden, um 2 Türen zu indizieren. Zu jeder Tür gibt es ein IN und ein OUT-Gerät (abhängiges Gerät). Lesen Sie in der Ingressus Einbauanleitung, wie Sie die Tür und abhängige IN- und OUT-Geräte definieren. Alles wird durch die Verkabelung zwischen Ingressus und den abhängigen Geräten kontrolliert.



Mit Rechtsklick auf die IP Adresse von Ingress können Sie den Anschluss umbenennen, zum beispiel Ingressus II - F&E Büro. Benennen Sie das abhängige Gerät (Slave) entsprechend seinem Modell eine für einfache Referenz.



Hinzufügen von Türschlössern (Keylocks) zu der Tür



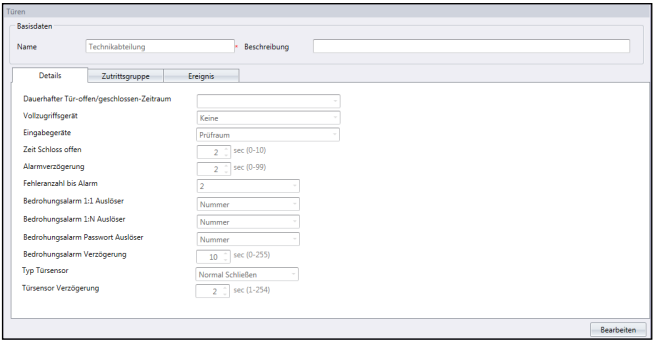
Ingress erzeugt automatisch eine Tür, benannt als Keylock 7700/8800, nachdem Sie das Gerät im Ingress System hinzufügen. Ingress fügt sofort das Gerät zu der Tür hinzu. Sie können das Gerät für eine einfache Referenz benennen.

Konfigurieren Sie die Einstellungen zu den Türen

Sie können die Zugangseinstellungen in Ingress konfigurieren und auf beide gekoppelte Geräte mit der Tür hochladen. Dies stellt sicher,dass beide standalon Geräte die gleichen Zugangseinstellungen während der Operation anwenden. Wenn Sie ein standalone Gerät und einen Slave benutzen, um die Tür zu sichern, werden die Einstellungen nur zum standalone Gerät gesendet.

Ingress behandelt Ingressus II als 2 verschiedenen Türen, auch wenn es nur von einem Gerät ist. Sie können die Zugangseinstellungen für jede Tür individuell konfigurieren. Ingressus II kann die Einstellungen zur Tür dementsprechen speichern und anwenden.

Ignorieren Sie dies, wenn Sie die Türschloss-Serie (Keylock) installieren. Aufgrund des nicht vorhandenen Kommunikationskabels, kann Ingress keine Einstellungen auf das Keylock hochladen.. Daher brauchen Sie in Ingress nichts konfigurieren.



1. Klicken Sie, um eine Tür zu wählen.
2. Drücken Sie auf Bearbeiten im rechten Fenster
3. ändern die Einstellungen entsprechend.

Allgemeines Einstellungen für standalone Gerät und Ingressus.

Tür permanent Offnen / Schließzeitraum: Wählen Sie einen Zeitraum, der den freien Zugang erlaubt (ohne Verifizierung am Gerät). Ratsam sind nur Bereiche mit öffentlichem Zugang während bestimmter Zeiten. Benötigen Sie keine öffentlichen Zugangszeiten, lassen Sie dieses Feld leer.

Öffnungsdauer des Schlosse: Hier können Sie den Zeitraum einstellen, den die Tür nach erfolgreicher Verifizierung geöffnet bleiben soll.

Sensortyp der Tür: Wählen Sie die Art des Türsensors, die im Gerät eingestellt wurde. Die häufigste Typ ist NC (Normal geschlossen). Türsensor ist ein wichtiger Bestandteil, wenn Sie die Türaktivitäten überwachen möchten. Er richtet sich immer nach dem Einzelgerät oder Ingress berichtet permanent den Türstatus.

Konfigurationen für Türen ausschließlich mit standalone Gerät

Gerät mit vollem Zugang: Wichtige Einstellung, wenn Sie Zeitzone-Einstellungen auf die Tür anwenden. Wählen Sie ein Ausgangsterminal , um einen Terminal mit jederzeitigem Zugang zu haben. Ein Gerät mit vollem Zugang ignoriert die Zeitzoneneinstellungen. Benutzer können sich auf diesem Gerät verifizieren, um den Bereich jederzeit zu verlassen.

Eingangs-Terminal: Eingangs-Terminal: Definieren Sie, ob das Gerät für In oder Out Transaktionen benutzt wird. Zum Beispiel, alle Datensätze vom "IN" Gerät werden als "Ankommen" eingetragen,und die Datensätze aus dem anderen Terminal werden an der gleichen Tür wird als "Verlassen" eingetragen.

Alarmverzögerung: Ändern, um die Dauer festzulegen, bevor der Alarm im Notfall auslöst. Setzen Sie auf 0, um das Gerät beim Notfall sofort auszulösen.

Fehler-Anzahl für Alarm: Um die maximale Anzahl der fehlgeschlagenen Verifikation festzulegen, bevor das Gerät den Alarm auslöst. Dies ist, um die unberechtigte Person zu warnen, das Gerät nicht weiter zu manipulieren.

Bedrohungsalarm 1:1 Auslöser

Bedrohungsalarm 1:N Auslöser

Bedrohungsalarm Passwort Auslöser: Nutzer können sich im Notfall an der Tür verifizieren, um Bedrohungsalarm auszulösen und andere zu warnen. Zum Beispiel, wenn ein Räuber den Benutzer zwingt, sich zu verifizieren, um Zugang in den Bereich zu erhalten. Der Nutzer kann dann den Alarm auslösen, um die Benutzer, die drinnen sind zu alarmieren.
Aktivieren Sie eine der oben genannten Möglichkeiten, Bedrohungsalarm auszulösen. Wenn Sie Fingerabdruck Verfizierung benutzen, um üblicherweise Zugang zu erhalten, aktivieren Sie Bedrohungsalarm Passwort. Das Gerät wird dann den Alarm auslösen, wenn Sie Ihr Passwort eingeben. Sehen Sie bitte in das Benutzerhandbuch des Gerätes für Details, wie Sie den Fingerabdruck oder das Passwort anmelden, um Bedrohungsalarm auszulösen.

Bedrohungsalarm Verzögerung: Stellen Sie die Dauer ein, bevor der Alaram während des Notfalls ausgelöst wird. Setzen Sie 0 und das Gerät wird während eines Notfalls sofort auslösen.

Sensortyp der Tür: Wählen Sie die Art des Türsensors aus, der auf dem Gerät eingestellt wurde. Üblich ist NC. Der Tür-Sensor ist ein wichtiger Bestandteil, um die Tür-Aktivitäten zu überwachen. Wenn die Tür mit dem Gewalt geöffnet wird oder die Tür bleibt offen, meldet sich der Türsensor bei dem Gerät. Sie können den Status der Tür auf der Seite der Überwachung bei Ingress ansehen. Wählen Sie "Keine" aus, wenn Sie keinen Tür-Sensor installieren haben. Sie können die Aktivitäten dieser Tür dann nicht überwachen.

Türkonfigurationen nur für Ingress

Tür permanent Offnen/ geschlossen in Urlaubzeiten: Wählen Sie einen Zeitraum, um freien Zugang (ohne Verifizieung am Gerät) in den Bereich während des Urlaub zu erlauben. Hierzu ist die Einrichtung einer Urlaubsliste und eines Urlaubszeitsraumes erforderlich. Dieses Feld leer lassen, um diese Merkale zu ignorieren.

Punch-Intervall: Richten Sie die Zeitdauer zwischen der ersten und zweiten Überprüfung desselben Benutzers ein, zum Beispiel, 10s. Ingressus wird dem Benutzer den Zugang verweigern, wenn er sich zweimal innerhalb von 10 Sekunden an irgendeinem Slave-Geräten verifiziert.

Verifizierungsmodus: Wählen Sie eine Kombination von Verifikation, um Zugang zu erhalten.

Bedrohungs-Passwort: siehe Bedrohnungsalarm

Notfallpasswort: Während des Notfalls können die Benutzer ein Notfallpasswort eingeben, um jederzeit jede Tür (durch Ingressus kontrolliert) zu entriegeln. Zeitzonen- oder Zugangskontrolleinstellungen werdenignoriert. Üblicherweise ist dies Aufgabe des Administrators.

Tür-Sensor Verzögerung: Stellen Sie die Zeitdauer ein, bevor Ingressus den Alarm auslöst, wenn die Tür offen stehen bleibt.

Sofortverschluss: Aktivieren Sie diesen, wenn das EM-Schloss oder Riegelschloss sofort sperren soll, sobald die Tür schließt. Sie müssen die Türsensoren zusammen mit dem Türschloss installieren. Wenn die Türsensoren einander berühren, erhält Ingressus das Signal und aktiviert sofort das Türschloss. Dies Funktion überschreibt die Einstellungen der Dauer des Türöffnens und kann unberechtigten Zutritt durch dichtes Aufschließen zum Vordermann vermeiden.

4. Speichern Einstellungen.
5. Hochladen neue Einstellungen zum Gerät.

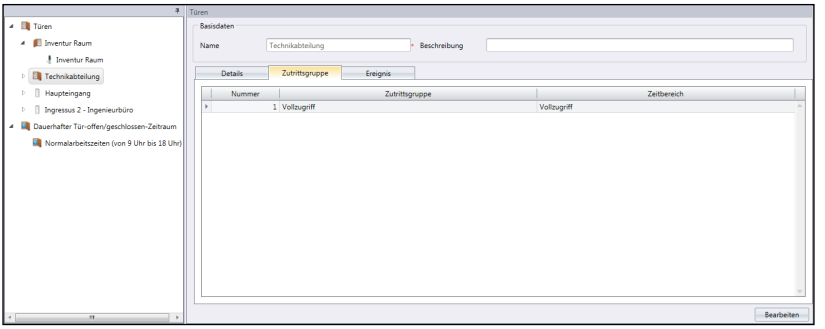
Löschen Gerät/Türen

Sie können die Geräte oder Türen löschen, wenn sie nicht mehr im Gebrauch sind. Stellen Sie sicher, dass Sie die Geräte und Türen identifizieren, bevor Sie mit dem Löschen fortfahren.

1. Klicken Sie auf ein Gerät oder eine Tür, die in der linken Leiste angezeigt werden, um sie zu entfernen.
2. Klicken Sie auf Gerät entfernen oder Tür entfernen um fortzufahren.
3. Klicken Sie auf Ja und bestätigen Sie das Löschen.

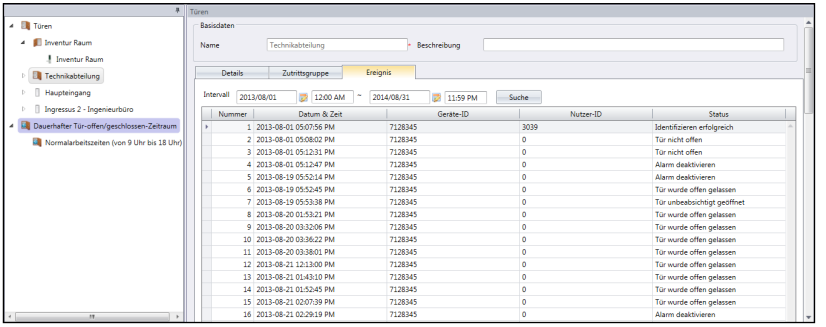
Zugangsgruppe der Tür

Sie können den Zugang eines jeden Benutzers für jede Tür und jeden Zeitraum beschränken. Zum Beispiel alle Benutzer können durch den Haupteingang eintreten, aber nur Verwaltungsmitarbeiter können in der Verwaltungsabteilung während Bürostunden eintreten. Beachten Sie Zugangsniveau für weitere Informationen.



Hier können Sie nur die Zugangszeitintervalls von jedem Benutzer für jede Tür anschauen. Sie können sie nur in der Berechtigungsstufe verändern.

Türereignisse


Türen
Inventur Raum
Inventur Raum
Technikabteilung
Haupteingang
Ingressus 2 - Ingenieurbüro
Dauerhafter Tür-offen/geschlossen-Zeitraum
Normalarbeitszeiten (von 9 Uhr bis 18 Uhr)
Basisdaten
Name
Technikabteilung
Beschreibung
Details
Zutrittsgruppe
Ereignis
Intervall
2013/08/01
12:00 AM
2014/08/31
11:59 PM
Suche
Nummer
Datum & Zeit
Geräte-ID
Nutzer-ID
Status
1 2013-08-01 05:07:56 PM 7128345 3039 Identifizieren erfolgreich
2 2013-08-01 05:08:02 PM 7128345 0 Tür nicht offen
3 2013-08-01 05:12:31 PM 7128345 0 Tür nicht offen
4 2013-08-01 05:12:47 PM 7128345 0 Alarm deaktivieren
5 2013-08-19 05:52:14 PM 7128345 0 Alarm deaktivieren
6 2013-08-19 05:52:45 PM 7128345 0 Tür wurde offen gelassen
7 2013-08-19 05:53:38 PM 7128345 0 Tür unbeabsichtigt geöffnet
8 2013-08-20 01:53:21 PM 7128345 0 Tür wurde offen gelassen
9 2013-08-20 03:32:06 PM 7128345 0 Tür wurde offen gelassen
10 2013-08-20 03:36:22 PM 7128345 0 Tür wurde offen gelassen
11 2013-08-20 03:38:01 PM 7128345 0 Tür wurde offen gelassen
12 2013-08-21 12:13:00 PM 7128345 0 Tür wurde offen gelassen
13 2013-08-21 01:43:10 PM 7128345 0 Tür wurde offen gelassen
14 2013-08-21 01:52:45 PM 7128345 0 Tür wurde offen gelassen
15 2013-08-21 02:07:39 PM 7128345 0 Tür wurde offen gelassen
16 2013-08-21 02:29:19 PM 7128345 0 Alarm deaktivieren

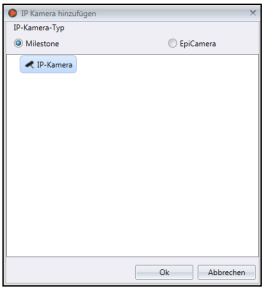
Jedes Gerät läd Aktivitäten (z.b.: Tür gewaltsam geöffnet) automatisch zu Ingress hoch. Sie können diese Berichte entsprechend zu Datum und Uhrzeit anschauen.

1. Drücken Sie auf Bearbeiten.
2. Definieren Sie die Datenreichweite Reichweite/Intervall.
3. Drücken Sie auf Get Log.

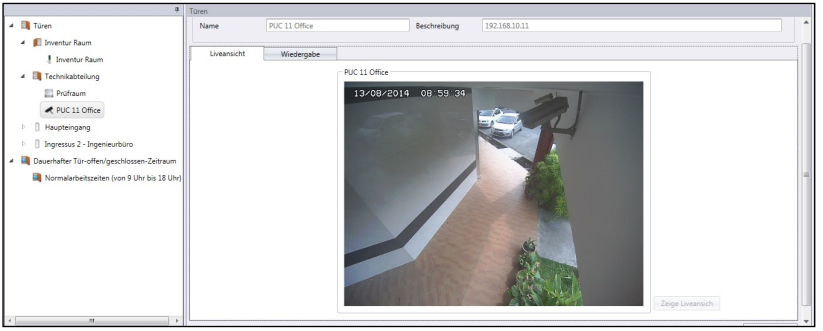
Verbindund mit IP Kamera

Ingress kann mit dem Milestone Server oder EpiCamera verknüpft werden, um Videos zu übertragen. Sie können Live-Ansichten von Ihrer IP Kamera in Ingress anschauen - ohne Anmeldung zu Milestone oder EpiCamera. Sie können die IP Kamera mit relevanten Türen verbinden, so dass Sie jedes Hineingehen und Verlassen leicht überwachen können.

Bevor Sie mit der verbindung einer IP Kamera zu einer Tür beginnen, gehen Sie auf System Einstellungen, um die Verbindingsdetails mit Ihrem Milestone Server oder Ihrer Epi-Camera unter Netzwerk Kamera Integration konfigurieren.



1. Wählen Sie Tür im linken Panel.
2. Klicken Sie auf Kamera hinzufügen.
3. Wählen Sie MileStone oder EpiCamera.
4. Wählen Sie die IP Kamera, die Sie mit der Tür verbinden wollen.
5. Die IP Kamera wird am linken Panel unter der ausgewählten Tür angezeigt werden.
6. Wählen Sie die IP Kamera und klicken Sie Live-Bild zeigen, um Video zu streamen.



Im Fall einer außergewöhnlichen TürAktivität (z.b.: Tür gewaltsam geöffnet), erfasst Ingress das Ereignis sofort unter Überwachung. Sie können das Viedo während der ungewöhnlichen Aktiviäten durch Anklicken der Alarmmeldung wiedergeben. Weitere Informationen unter Überwachung.

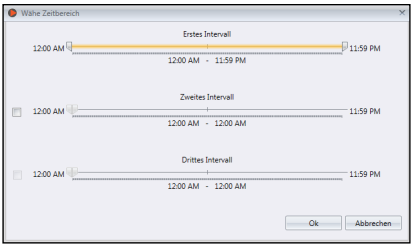
1. Wählen Sie Ip Kamera vom linken Panel aus.
2. Klicken Sie an Kamera entfernen.
3. Klicken Sie Ja, um zu bestätigen des Löschens.

Tür permanent Öffnen oder Schließen Zeitzone

Sie können eine bestimmte Zeitbereich aufstellen, um freien Zugang für einen bestimmten Eintitt zu erlauben, zum Beispiel, Verkaufsbüro wird für Kunden geöffnet, um es während der Öffnungszeiten (9 Uhr bis 17 Uhr) zu besuchen. Benutzer brauchen keine Verifizierung, um Zugang von 9 Uhr bis 17 Uhr zu erhalten. Dies wird als Tür permanent Öffnen oder Schließen Zeitzone bezeichnet, gestalted um Zugang für Zonen mit hohem Durchgangsverkehr zu kontrollieren, ohne den Sicherungszweck zu beeinträchtigen.

Schritt für Schritt Tür permanent Öffnen Schließen Zeitzone:

1. Klicken Sie auf Tür permanent Öffnen Schließen Zeitzone.
2. Klicken Sie auf Zeitzone hinzufügen.
3. Name die Zeitzone, z.b: Öffnungszeit - freier Zugang von 9 uhr bis 16 uhr.
4. Drücken Sie Bearbeiten.
5. Definieren Sie Start und Schluss Zeit für jeden Tag.
   - *Sie können auf die Schaltfläche kopieren klicken, um die Einstellungen des vorherigen Tages zu kopieren.*
   - *Klicken Sie [..], um Zeiträume durch Rollbalken zu definieren.*



6. Drücken Sie [Speichern] um die Einstellungen zu speichern.

Schritte um Tür permanent Öffnen Schließen Zeitzone zur Tür zuzuweisen:

1. Wählen Sie bitte Tür aus der linken Leiste.
2. Wählen Sie Details.
3. Drücken Sie Bearbeiten.
4. Wählen Sie die Zeitzone unter Tür permanent Öffnen Schließen Zeitzone.
5. Drücken Sie auf Speichern.
6. Übertragungseinstellungen zu Geräten.

Um die Permenant Tür geschlossen Zeitzone von der Liste entfernen:

1. Wählen Sie die Zeitzone im linken Fenster.
2. Klicken Sie auf Entfernen Zeitzone.
3. Bestätigen Sie Ja zum löschen.

Tür permanent Öffnen Schließen Urlaub Zeitzone. (nur für Ingressus)

Sie können während des Urlaubs eine dauerhafte Türschluss Zeitzone anwenden. Ingress verwendet die Zeitzoneneinstellungen mit dem Datum, wie unter Urlaubseinstellungen angegeben. Es ist nur an den Türen möglich, die mit Ingressus installiert sind.

Schritt für Schritt dauerhafte Tür Öffnen Schließen Zeitzone:

1. Klicken Sie Dauerhaft Tür Öffnen Schließen Zeitzone.
2. Klicken Sie hinzufügen Sie Urlaub Zeitzone.
3. Name die Zeitzone, z.b.: Urlaub Zugang - nur Morgens.
4. Drücken Sie Bearbeiten.
5. Geben Sie Begin und Endzeit ein.
6. Drücken Sie Begin und Endzeit.

Schritt zum Permanent Tür Öffnen Schließen Urlaub Zeitzone zu Ingressus:

1. 1. Wählen Sie Ingressus im linken Fenster.
2. Wählen Sie Details.
3. Drücken Sie Bearbeiten.
4. Wählen Sie Zeitzone unter Permanente Tür Öffnen Schließen Urlaub Zeitzone.
5. Drücken Sie Speichern.
6. Übertragungseinstellungen zum Ingressus.

Um Permanent Tür Öffnen Schließen Urlaub Zeitzone von Liste zu entfernen:

1. Wählen Sie Urlaub Zeitzone im linken Fenster.
2. Klicken Sie löschen Sie Urlaub Zeitzone.
3. Bestätigen Sie Ja zum löschen.

Kapitel 3

Einstellung der Zonen

In diesem Kapitel wird erläutert, wie Sie Zoneninstallationen unter Nutzung von Ingressus vornehmen.

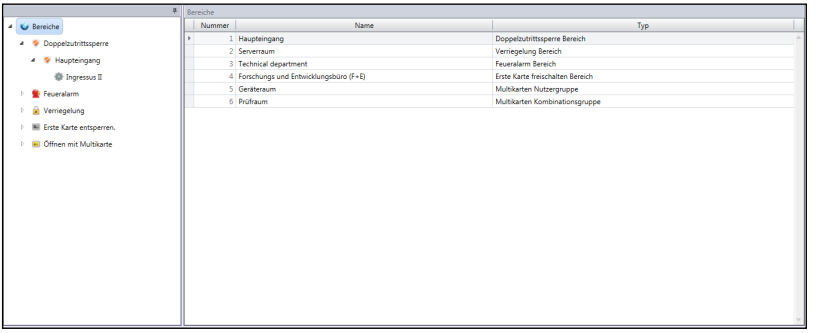
Dieses Kapitel ist nur für Ingressus anzuwenden. Überspringen Sie dieses Kapitel, wenn sie keine Ingressus Kontroller in Ihrer Umgenung installieren. Sie können Zoneninstallation mit Ingressus einstellen, um mehr sichere Zugangskontelleinstellungen auszuführen.

Es gibt ingesamt 5 Arten von Zonen, die sind:

- Antipassback
- Feueralarm
- Interlocking (Ineinandergreifend)
- Wächterfunktion
- Vier-Augen-Prinzip
- Antipassback (Einschleichschutz)

Antipassback

Wenden Sie Antipassback (Einschleichschutz) an, um alle Benutzer zu zwingen sich jederzeit wann sie "ankommen" oder "den Arbeitsplatz verlassen", zu verifizieren. Ingressus sperrt Benutzerzugänge, wenn der Benutzer seine vorherige Verifizierung verpasst hat. Das ist eine wichtige Eigenschaft, um zu verhindern, dass ein Benutzer sich durch dichtes Aufrücken auf den Vordermann Zugang verschafft (einschleicht). Ingress kann die vollständigen In-Out Protokolle aller Benutzer sammeln.



1. Klicken Sie auf Antipassback im linken Fenster
2. Klicken Sie Zone hinzufügen.
3. Name die Zone, z.b.: Erdgeschoss
4. klicken Sie Gerät hinzufügen.
5. Wählen Ingressus von der Liste.
6. Name des Ingressus Kontroller.
7. Drücken Sie Bearbeiten in dem Fenster Basisinformationen.

8. Wählen Sie die Art des Antipassbacks durch klicken auf dem Schaltknopf

   Antipassback zwischen Leser der Tür 1:, um Eigenschaften nur an der Tür 1 zu aktivieren.

   Antipassback zwischen Leser der Tür 2:, um Eigenschaften nur an der Tür 2 zu aktivieren.

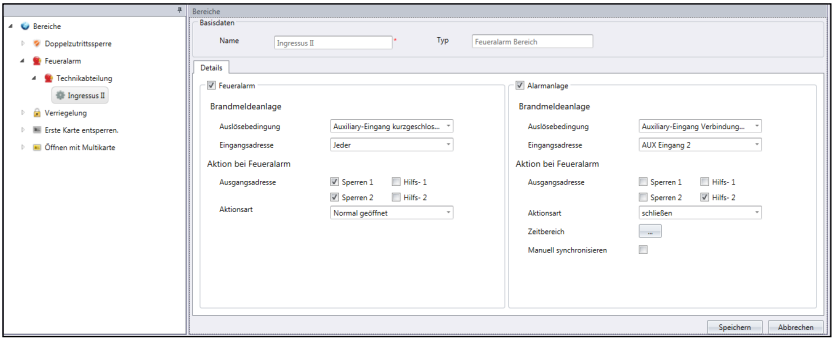
   Antipassback zwischen den Lesern von Tür 1 und den Lesern der Tür 2 jeweils: um die Eigenschaften an Tür 1 und Tür 2 selbstständig zu aktivieren.

   Antipassback zwischen Tür 1 und Tür 2: Um de Merkmal zwischen den beiden Tür 1 und Tür 2 zu aktivieren. Benutzer muss den Ausgang Datensatz von der Tür 1 haben, bevor den Zugang zu 2. Tür gewährt.

9. Synchronisation der Einstellungen zum Ingressus Kontroller.

Feuer und Einbruchalarm

Wenden Sie Feueralarmeinstellungen in Ingressus an, um Benutzer im Falle eines Brandes zu alarmieren. Sie müssen den AUX Eingang an Ingressus (z.b.: Rauch/Hitze Melder) installieren. Der Sensor schickt Signale zu Ingressus, sobald er Rauch / Hitze aufdeckt. Sie können in Ingress konfigurieren, dass Ingressus die Türen sofort entriegelt.



1. Klicken Sie Feueralarm im linken Fenster.
2. Klicken Sie Zone hinzufügen.
3. Name die Zone, z.b.: alle Türen.
4. Klicken Sie Gerät hinzufügen.
5. Wählen Ingressus von der Liste.
6. Name des Ingressus Kontrollers.
7. Drücken Sie bearbeiten im Detail Fenster.
8. Bestätigen Sie das Feueralarm Kästchen, um die Konfiguration zu starten.

   Auslösesignale: Um die Signale zu definieren, die Brandalarm in Ingressus auslösen . Es können entweder Sensoren (zum AUX Port an Ingressus verbinden) oder Schlüsselbefehle der abhängigen Terminals (Slave) (setzen Sie besondere Passworte ein, Verifizierung mit Bedrohungsfinger. Zum Beispiel, wählen Sie Auxiliär Input Shorted, wenn Sie Rauch/Hitze Sensoren benutzen, um Feuer zu aufspüren. Der Sensor verbindet sich zu Ingressus an seinem AUX Eingangs-Port. Es schickt Signale nur zu Ingressus, wenn er Rauch oder Hitze aufspürt.

Eingangspunkt-Adresse: Um die Art des Eingangs zu Ingressus zu definieren,der Brandalarm auslöst. Wählen Sie als Eingang irgendein abhängiges Geräte (Slave), das Sie benutzen, oder Hilfs-Input Port 1 und 2. Sie werden nur einen Hilfs-Input Port 1 finden, wenn Sie Ingressus I installieren.

9. Konfigurieren Sie die Ausgabe von Ingress während Feueralarm.

   Ausgangspunkt Adresse: Definiert die Art der Aktion von Ingressus während eines Feueralarms, entweder Verschluss oder Auxiliär Output. Bestätigen Sie Verschluss 1 und 2, wenn Sie den Türverschluss während des Feueralarms steuern möchten. Wählen Sie Auxiliär 1 und 2 , wenn Sie einen Sensor mit Auxiliär Output verbinden möchten.

   Aktiontyp: Definieren Sie Geschlossen, Geöffnet oder Normal Geöffnet als Output von Ingressus.
   Geschlossen *- Ingressus sendet ein NC Relaissignal vom AUX Port. Die NC Relaissignal kann die Schaltung eines anderen Kreises aktivieren, z.b.: Sirene anstellen um die Nutzer zu warnen.*

   Offen *- Ingressus gibt NO Relaissignal von AUX-Port. Die NO Relaissignal kann die Schaltung eines anderen Kreises abschalten, z.b.: Abschalten der Stromversorgung des Türschlosssystems.*

   Wenn Sie Geschlossen 1 und 2 unter Ausgabepunkt Adresse ausgewählt haben, wählen Sie öffnen, um die Türen während Brandmeldung zu öffnen.

   Verzögerung *-Die Wartezeit, bis die Aktion startet.*

10. Einstellungen der Synchronisation zum Ingressus Kontroller.

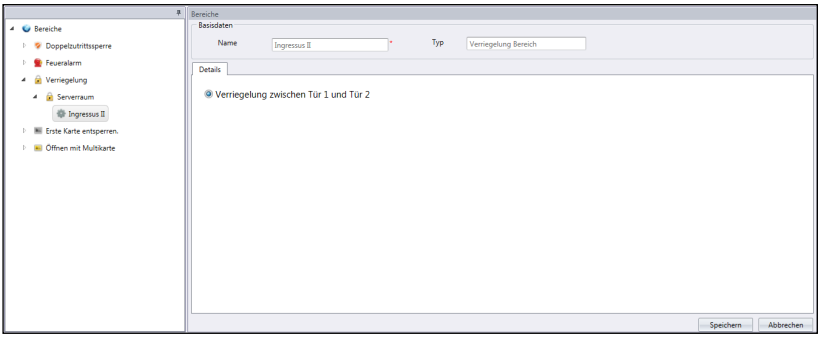
Ingress kann mit Bewegungsmeldern verbunden werden, um Zonen nach Betriebsstunden zu überwachen. Im Falle eines Einbruchs, spürte der Bewegungsmelder die Bewegungen des Eindringlinges, und löst ein Alarmsignal aus. Im Gegensatz zu Rauch- und Brandmeldern müssen Bewegungsmelder ausgeschaltet werden, wenn der Zutritt in die Zone erlaubt ist. Anstatt einer manuellen Schaltung können Sie eine Zeitschaltung zu Aktivierung & Deaktivierung der Bewegungsmelders einstellen.

1. Bestätigen Sie das Einburchalarm Kästchen, um die Konfiguration zu starten.
2. Wählen Sie Hilfseingang Unterbrochen unter Auslösesignale
3. Wählen Hilfs Eingabe 2 als Eingangspunkt- Adresse (wir empfehlen, verbinden Sie Bewegenungsdetektor zu AUX IN Port 2).
4. Wählen Auxiliär 2 unter der Ausgangpunkt- Adresse (wir empfehlen AUX OUT 2 zum Anschluss zu Alarmsystem oder Sirene).
5. Wählen Schließen unter Aktiontyp
6. Synchronisation der Einstellungen der Ingress Kontroller

Interlocking (Ineinandergreifend)

Dies wird auch als Falle bezeichnet und ist nur für die Installation von Ingressus II mit 2 Türen anwendbar. Mit dieser Einstellung ist Ingressus in der Lage, festzustellen, ob die Tür fest geschlossen ist, bevor der Benutzer sich zum Öffnen der nächsten Tür verifiziert.

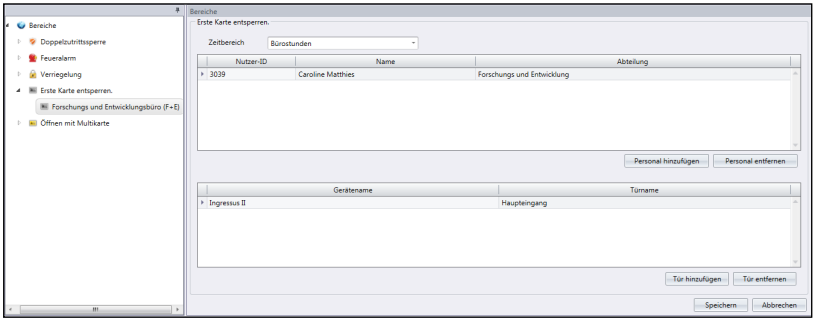
1. Klicken Sie auf Ineinandergreifen im linken Fenster.
2. Klicken Sie auf Zone hinzufügen.
3. Name Die Zone, z.b.: Serverräume.
4. Klicken Sie Gerät Hinzufügen.



5. Wählen Ingressus aus der Liste
6. Name des Ingressus Kontrollers.
7. Drücken Sie Bearbeiten im Detail Fenster.
8. Bestätigen Sie Verriegeln zwischen Tür 1 und Tür 2 um die Funktion zu aktivieren.
9. Drücken Sie Speichern, um Einstellungen zu speichern .
10. Synchronisation der Einstellungen mit dem Ingressus Kontroller.

Wächterfunktion

Sie können einen Benutzer/ Karte als "Wächter" einsetzen, wobei sich erst dieser Benutzer / Karte verifizieren muss, bevor anderen der Zugang zu diesem Bereich geben werden kann. Wenn der "Wächter" für die Verrifizierung nicht verfügbar ist, können andere Benutzer können keinen Zugang erhalten. Dieser Funktion stellt in sensiblen Bereichen sicher, dass der Verantwortliche anwesend ist, um den Bereich zu beobachten, bevor andere Benutzer den Zugang erhalten.

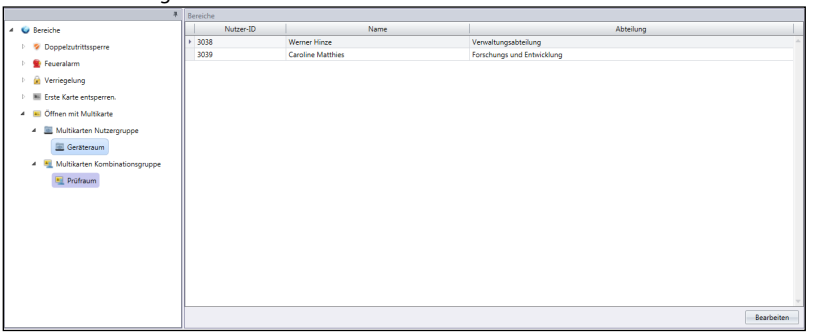


1. Klicken Sie auf Wächterfunktion im linken Fenster.
2. Klicken Sie Zone Hinzufügen.

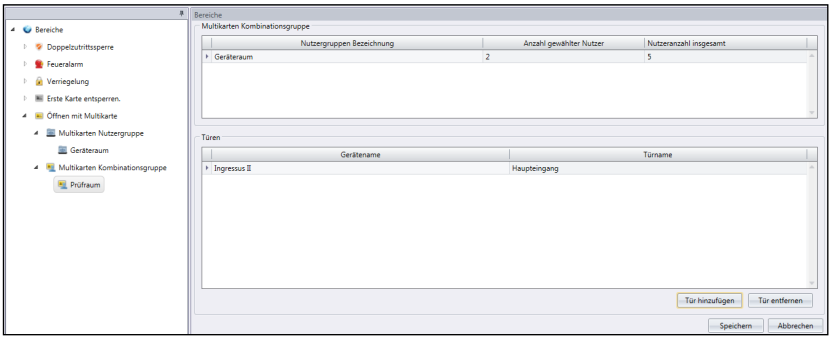
3. Name der Zone, z.b.: F&E Büro.
4. Klicken Sie hinzufügen Gerät.
5. Wählen Sie Ingressus von der Liste.
6. Name des Ingressus Kontrollers
7. Drücken Sie Bearbeiten im Fenster der Zone
8. Wählen Sie Zeit bestimmen,um Zeitraum für "Wächterfunktion" festzulegen. Außerhalb dieses Zeitraums gibt es keine Zutrittsberechtigung.
9. Klicken Sie auf Hinzufügen Personal um den Benutzer als Wächter zu benennen (er/sie kann zur verifizierung Karte, Passwort oder Fingerabdruck verwenden). Sie können mehr als 1 Wächter benennen.
10. Klick Tür hinzufügen um festzulegen, welche Ingressus Kontroller dieser Regel folgen sollen.
11. Drücken Sie Speichern um die Einstellungen zu speichern
12. Synchronisation der Einstellungen zum Ingressus Kontroller

Vier-Augen-Prinzip

Das Vier-Augen-Prinzip ist eine Sicherheitsfunktion, bei der die Türen nur entriegeln, wenn sich mindestens 2 spezifierte Benutzer gleichzeitig an der Tür verifizieren, um Zugang zu erhalten. Sie können bis zu maximal 5 Benutzer einstellen, die sich verfizieren müssen, um eine Tür zu entriegeln.



1. Klicken Sie Vier-Augen-Prinzip.
2. Klicken Sie Benutzergruppe hinzufügen.
3. Name die Benutzergruppe z.B: F&E Gruppe.
4. Klicken sie Bearbeitung im rechten Feld.
5. Wählen die entsprechenden Benutzer aus der Liste.
6. klicken Sie auf Speichern um die Einstellungen zu speichern.
7. Klicken Sie auf Vier-Augen Kombination Gruppe im linken Fenster.
8. Klicken Sie auf Kombination Gruppe hinzufügen.
9. Name Name der Kombination Gruppe z.b.: Sperrgebiet - Niveau 1.



10. Drücken Sie auf Bearbeiten, um die Konfiguration zu starten.
11. Doppelklicken Sie auf die Nummer des ausgewählte Benutzer, um ihn dieser Gruppe zuzuweisen.
12. Drücken Sie Tür hinzufügen, um auszuwählen , welcher Ingressus Kontroller dieser Regel folgen soll.
13. Drücken Sie Speichern, um die Einstellungen zu speichern.
14. Synchronisation zum Ingressus Kontroller.

Löschen Zone/Gerät/Benutzer Gruppe/ Vier-Augen-Gruppe.

Sollte eines der obengenannten nicht in Ihrer Umgebung anwendbar sein, oder wenn Sie fälschlicherweise eine Konfigurationen in der Liste hinzugefügt haben, können Sie diese aus der Liste, wie folgt löschen:

1. Wählen die entsprechende Zone/Gerät/Benutzergruppe/ Vier-Augen-Gruppe, die gelöscht werden soll, aus dem linken Fenster.
2. Klicken Sie den Button in der oberen Menüleiste (Entfernen Sie Zone, Löschen Sie Gerät, Löschen Sie Benutzergruppe oder Vier-Augen-Gruppe).
3. Klicken Sie auf Ja, um Löschen zu bestätigen.

beziehungsweise:

1. Wählen Sie das zu löschende Element.
2. Rechtklick auf das Element, um löschen zu wählen.
3. Klicken Sie auf Ja, um Löschen zu bestätigen.

Kapitel 4

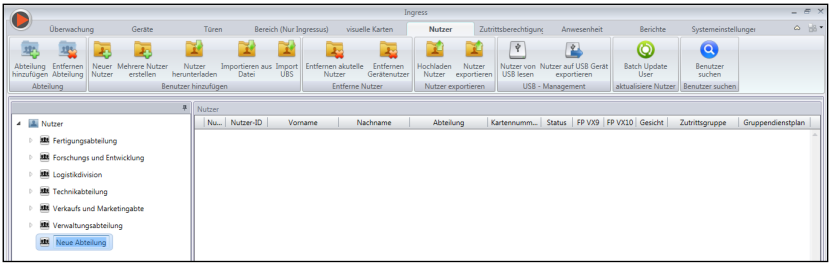
Nutzerverwaltung

Dieses Kapitel zeigt Ihnen, wie Sie die Benutzer durch Synchronisierung von den Geräten mit Ingress verwalten und wie Sie detailierte Benutzerinformation für die Berichterstattung ausfüllen.

Synchronisieren Sie alle Benutzer von den Geräten mit Ingress für eine einfache Verwaltung. Sie können alle wichtigen Information über jeden Benutzer als Referenz ausfüllen und die Informationen des Benutzers zu allen Geräten übertragen, um entsprechenden Zugang zu erlauben. Der Übertragungsprozess benötigt eine TCP/IP oder RS485 Verbindung zu jedem Gerät. Wenn diese Kommunikationsmethode nicht verfügbar ist, können Sie die Informationen des Benutzers auf einem USB-Stick kopieren, um die Information zwischen Ingress und dem Gerät zu übertragen. Sie können die Informationen des Benutzers von Ihrem aktuellen System in Ingress importieren, so dass Sie die Information erneut einzugeben brauchen.

Abteilung hinzufügen

Erstellen Sie eine Liste von Abteilungen in Ingress, bevor Sie die Benutzern synchronisieren oder erstellen.



1. Klicken Sie auf Benutzer im linken Fenster.
2. Klicken Sie auf Abteilung hinzufügen.
3. Name der Abteilung.

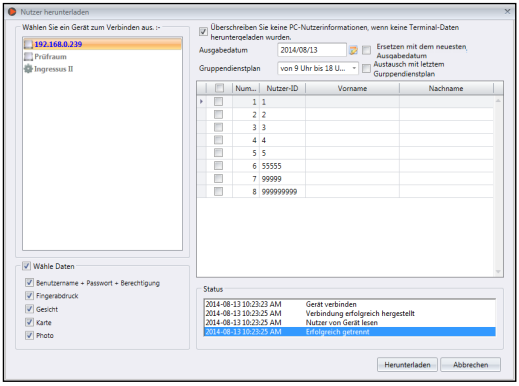
Benutzer hinzufügen

Die Benutzer von Geräten herunterladen.

Der leichteste Weg, um Benutzer hinzuzufügen ist, Benutzer aus den Geräten zu synchronisieren. Hierfür lesen Sie die Benutzer mit Gesicht, Fingerabdruck, Karte und Passwort zuerst im Terminal ein.

Starten Sie dann Ingress, um die Benutzer herunterzuladen und unter einer Abteilung entsprechend zuzuweisen. *Beachten Sie Kapitel 4 • um Personaldaten des Benutzers von einem anderen System zu importieren,* um zu erfahren, wie die Personaldaten des Benutzers aus einem Drittsystem importiert werden ,so dass Sie die Personaldaten nicht manuell eingeben müssen.

1. Klicken Sie auf Benutzer herunterladen in der Menüleiste
2. Doppelklick um das Gerät im linken Fenster zu wählen.
3. Bestätigen Sie das Anwahlfeld, um Benutzerdaten herunterzuladen.



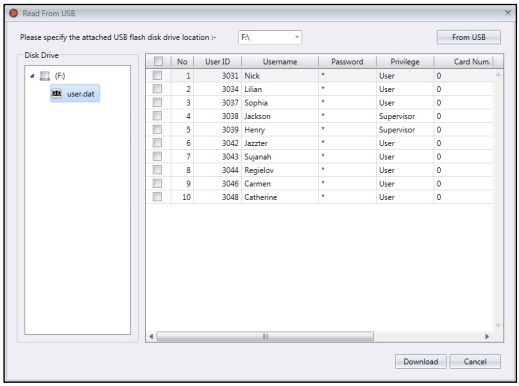
Benutzername + Passwort + Privileg (Pflichtelemente. Ingress ignoriert Benutzername und Passwort , wenn der Benutzer diese nicht eingelesen hat.
Fingerabdruck (wählen Sie nur, wenn Sie den Fingerabdruck des Benutzers herunterladen wollen)
Gesichtsvorlage (wählen Sie nur, wenn Sie die Gesichtsvorlage des Bunutzers herunterladen wollen)
Karte (wählen Sie nur, wenn Sie die Karten-ID des Benutzers herunterladen wollen.

4. Bestätigen Sie "Überschreibe keine PC Benutzer Info, wenn keine Terminal Daten heruntergeladen wurden". So vermeiden Sie, dass versehentlich leere Daten vom Gerät heruntergeladen werden. Ingress wird anderenfalls alle Benutzerdaten von seiner Liste löschen, wenn das angeschlossene Terminal leer ist. Ignorieren Sie dies, wenn Sie keine gespeicherten Daten in Ingress haben.
5. Wählen Sie die Benutzer aus dem rechten Fenster zum herunterladen.
6. Klicken Sie auf Herunterladen, um fortzufahren.

Um die Benutzer mit USB-Stick herunterzuladen.

Sie können einen USB-Stick nutzen, um Benutzer von allen Terminals und der Türschloss-Serie (Keykock) herunterzuladen. Nur der Ingressus Kontroller hat keine USB-Anschluss, um Daten zu übertragen.

1. Klicken Sie auf Lesen Sie Benutzer vom USB.
2. Klicken Sie zur Auswahl das USB Laufwerk mit dem der USB-Stick angeschlossen ist.
3. Klicken Sie auf vom USB.
4. Wählen Sie die Benutzer durch Klicken der Benutzer-ID.
5. Klicken Sie auf herunterladen, um die Daten der Benutzer in Ingress zu kopieren.



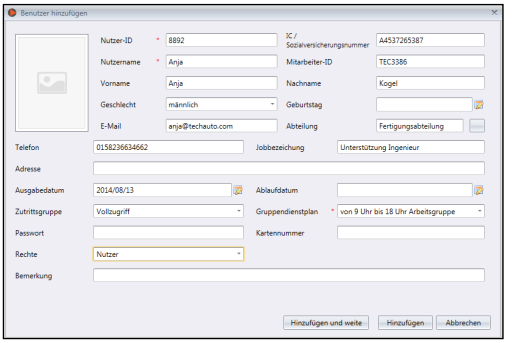
Manuelles Erstellen von Benutzern

Sie müssen die Benutzer im Ingress manuell generieren, wenn nur ein Ingressus Kontroller in der Umgebung installiert wurde, weil Sie nicht Fingerabdruck des Benutzers, Passwort oder Card-ID direkt in Ingressus einlesen können. In diesem Falle lesen Sie den Fingerabdruck in Ingress mit dem OFIS-Y Scanner (Fingerabdruck) ein, oder setzen Sie Passwort oder Kartennummer von jedem Nutzer in Ingress ein.

Sie können die Nutzer in einem Stapel mit fortlaufender Benutzer-ID für jede Benutzer anlegen. Wenn Sie zu jedem Benutzer eine RFID-Karte zuweisen, wo die Kartennummer der Reihe nach geordnet sind, können Sie die Benutzer im Stapel anlegen.

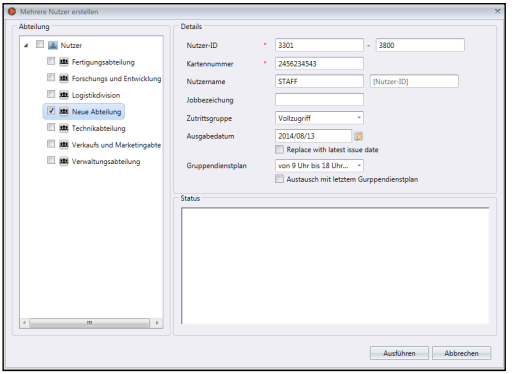
Um Benutzer nacheinander einzeln hinzufügen:

1. Klicken Sie auf Neuer Benutzer.
2. Füllen Sie die Personaldaten des Benutzers aus.
3. Klicken Sie auf hinzufügen und fortsetzen, um weitere Nutzer hinzuzufügen.
4. Beachten Sie 4.3.1, um zu erfahren, um wie Fingerabdrücke durch OFIS-Y Scanner eingelesen.



Benutzer im Stapel (in einem Vorgang) hinzufügen:

1. Definieren Sie Anfangs- und End-Benutzer-ID.
2. Stellen Sie die erste Kartennummer bereit, wenn Benutzer Karten mit fortlaufenden Sequenznummer benutzen.
3. Definieren Sie einen generellen Benutzername, um ihn mit einer Benutzer-ID zu verbinden, zum Beispiel “Staff1234”. Sie können später den Benutzernamen entsprechend abändern.

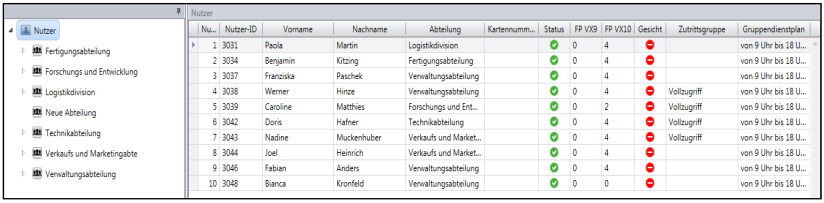


4. Erstellen Sie eine Bezeichnung, wenn alle Benutzer die gleiche Position teilen. Unterlassen Sie das, wenn sie verschiedenen Bezeichnungen haben.
5. Drücken Sie Ausführen um Benutzer zu erstellen.

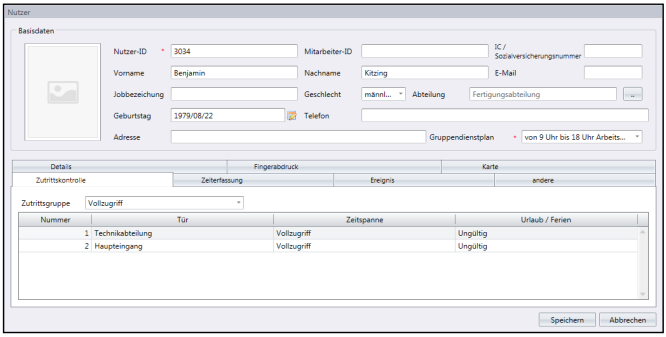
Bearbeiten von Personaldaten der Benutzer

Übertragen Sie die Benutzer in die Abteilung mit “Drag and Drop” (D&D). Füllen Sie die Personaldaten von jedem Benutzer aus, um die Suche in der Zukunft zu erleichtern. Sie können den einzelnen Benutzer auch manuell bearbeiten oder die relevanten Information von Ihrem vorherigen System in Ingress importieren.

Um Information des Benutzers manuell zu bearbeiten.


Nutzer
Nutzer
Fertigungsabteilung
Forschungs und Entwicklung
Logistikdivision
Neue Abteilung
Technikabteilung
Verkaufs und Marketingabte
Verwaltungsabteilung
Nu... Nutzer-ID Vorname Nachname Abteilung Kartennumm... Status FP VX9 FP VX10 Gesicht Zutrittsgruppe Gruppendienstplan
1 3031 Paola Martin Logistikdivision 0 4 von 9 Uhr bis 18 U...
2 3034 Benjamin Kitzing Fertigungsabteilung 0 4 von 9 Uhr bis 18 U...
3 3037 Franziska Paschek Verwaltungsabteilung 0 4 von 9 Uhr bis 18 U...
4 3038 Werner Hinze Verwaltungsabteilung 0 4 Vollzugriff von 9 Uhr bis 18 U...
5 3039 Caroline Matthies Forschungs und Ent... 0 2 Vollzugriff von 9 Uhr bis 18 U...
6 3042 Doris Hafner Technikabteilung 0 4 Vollzugriff von 9 Uhr bis 18 U...
7 3043 Nadine Muckenhuber Verkaufs und Market... 0 4 Vollzugriff von 9 Uhr bis 18 U...
8 3044 Joel Heinrich Verkaufs und Market... 0 4 von 9 Uhr bis 18 U...
9 3046 Fabian Anders Verwaltungsabteilung 0 4 von 9 Uhr bis 18 U...
10 3048 Bianca Kronfeld Verwaltungsabteilung 0 0 von 9 Uhr bis 18 U...

Sie können alle Benutzer im rechten Fenster sehen. Doppelklicken Sie auf die Benutzer-ID, um mit der Bearbeiten der entsprechenden Personaldaten zu starten.



1. Drücken Sie auf Bearbeiten.
2. Doppelklicken Sie auf Fotospalte, um sein/ihr Foto hochzuladen.
3. Füllen Sie die Details unter den Eckdaten aus, um den Benutzer zu beschreiben.
4. Klicken Sie auf jeden Reiter, um unter die Eckdaten anzuschauen oder zu konfigurieren.

- Details Tab

Benutzername: Kurzname, der während der Verifizierung zu Benutzer zu angezeigt wird. Maximal 9 Zeichen.
Passwort: Ein Passwort zur Verifizierung des Benutzers am Gerät. Maximal 5 Zeichen.
Ausstellungsdatum: Zeigt das Datum, an dem der Benutzer in Ingress erstellt wurde.
Ablaufdatum: Das Datum zu dem der Nutzer aus der Berechtigungsliste ausscheidet.
Sperren: Sperren des Zugangs des Benutzers, zum Terminal.
Privileg: Um das Privileg des Benutzers an den Geräten zu ändern.
Karte: Um die Kartennummer zu zeigen, die dem Benutzern zugewiesen ist.

Gesicht: Um zu zeigen, dass der Benutzer mit Gesichtsvorlage erfasst ist.
Insgesamt FP VX 9: um die Totale Anzahl der VX 9.0 Fingerabdruck Schablonen eingetragen für die Benutzer darzustellen.
Gesamtzahl FP VX 10: Zeigt die Gesamtanzahl der mit VX 10.0 eingelesenen Fingerabdrücke des Benutzers.

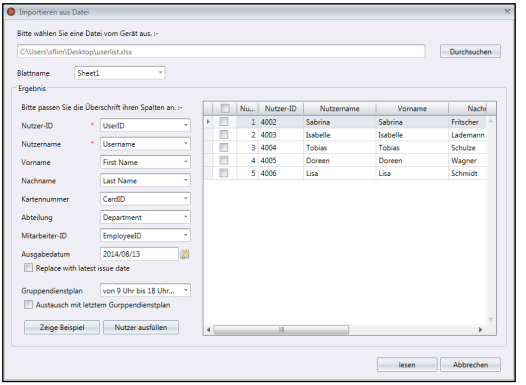
- Fingerabdruck Tab: Sie können einen neuen Fingerabdruck für Benutzer durch OFIS - Y Scanner unter FP VX 9.0/VX 10.0 einlesen. Folgen Sie unterstehenden Anweisungen:
  1. Stecken Sie den OFIS-Y Scanner in den Ingress Server/Client.
  2. Klicken Sie auf Benutzer-ID, um den Fingerabdruck einzulesen.
  3. Öffnen Sie die Seite FP VX 10 (Wenn Sie eine älteren Version, die VX 9.0 Fingerabdruck unterstützt, benutzen, öffnen Sie bitte FP VX 9, bevor Sie mit dem nächsten Schritt fortfahren.
  4. Drücken Sie auf Bearbeiten.
  5. Drücken Sie auf Anmeldung.

  Befolgen Sie die Anweisungen auf dem Bildschrim, um Fingerabdruck anzumelden.
- Card tab: Sie können eine neue Kartennummer für den Benutzer zuweisen / aktualisieren oder die Kartennumer der Benutzer entfernen.
  1. Klicken Sie auf Bearbeiten.
  2. Klicken Sie auf hinzufügen/aktualisieren/löschen.
  3. Synchronisieren Sie die Einstellungen zum Terminal.
- Zugangskontroll Tab: Diese Tabelle zeigt die Liste der Terminals, die diesen Benutzer zugewiesen sind.
- Anwesenheitszeit Tab: Diesee Tabelle zeigt den Stundenplan, der diesem Benutzer zugewiesen ist.
- Ereignis Tab: Sie können in dieser Tabelle die Zutrittsprotokolle des Nutzers anschauen. Definieren Sie Anfangs- und Enddaten, um Datensatz zu sehen.

Um Personaldaten des Benutzers aus einem anderem System zu importieren

Sie können Personaldaten des Benutzer aus anderem Systemen importieren, so dass Sie die Details nicht nochmal in Ingress eingeben müssen. Die importierte Datei kann in XLS, TXT oder CSV Format sein. Die Daten beinhalten:

- Benutzer-ID
- Benutzername
- Vorname
- Nachname
- Kartennummer
- Abteilung
- Mitarbeiter-ID



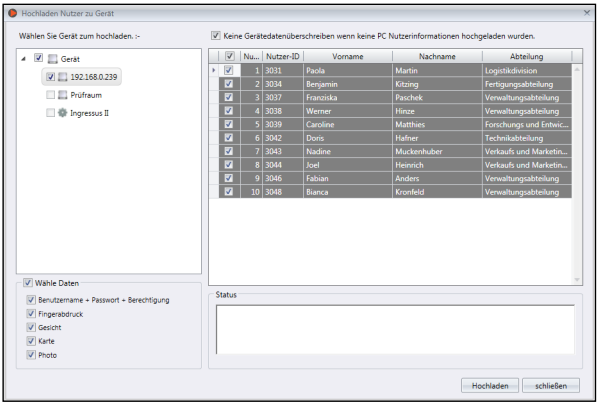
Es wird empfohlen, die Daten entsprechend der oben erwähnten Anordnung vorzubereiten. Sie können jedoch Ingress so konfigurieren, die Daten aus den bestimmnten Spalten auszulesen,um die Daten durch die folgende Schritte anzupassen:

1. Klicken Sie auf Durchsuchen, um die Datei zu finden oder zu öffnen.
2. Wählen Sie anpassen der Spalte der in Ingress zu importierenden Daten.
3. Klicken Sie auf Benutzer anzeigen, um die Daten zu sehen.
4. Klicken Sie auf Lesen, um den Import zu starten.

Nutzer auf Gerät hochladen

Sie können die Information des Benutzer auf das terminal ohne erneutes Einlesen des Benutzers hochladen. Sie können das via TCP/IP , RS485 oder USB-Stick hochladen.

Hochladen der Benutzer TCP/IP oder RS485



1. Klicken Sie auf Hochladen Benutzer.
2. Wählen Sie die Geräte im linken Fenster, um die Benutzer Informationen hochzuladen.
2. Ankreuzen des Anwahlfeldes , um Benutzer Information zum Hochladen auszuwählen.

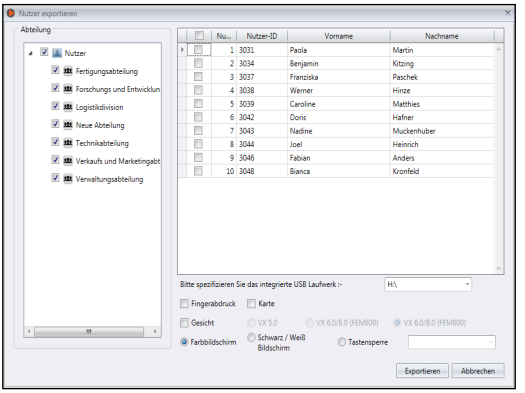
   Benutzername + Passwort + Privileg (Pflichtelemente. Ingress ignoriert Benutzername und Passwort , wenn der Benutzer diese nicht eingelesen hat.

   Fingerabdruck (wählen Sie nur wenn Sie den Fingerabdruck des Benutzers herunterladen wollen).

   Gesicht (wählen Sie nur, wenn Sie die Gesichtsvorlage des Bunutzers herunterladen wollen).

   Karte (wählen nur wenn Sie die Benutzer Karten ID herunterladen wollen).
4. Bestätigen Sie "Überschreiben Sie keine Terminal Daten, wenn keine PC Benutzer Info hochgeladen wird, um zu vermeiden, dass leere Daten auf das Gerät versehentlich hochgeladen werden. Ingress wird alle Benutzer Information im Terminal löschen, wenn Sie die in Punkt 3 erwähnten Information vergessen haben, einzubeziehen. Ignorieren Sie dies, wenn Sie sicher sind, dass das Gerät neu ist und keine Daten dort gespeichert sind.
5. Wählen Die Benutzer die aus dem rechten Fenster hochgeladen werden sollen.
6. Klicken Sie auf Hochladen um fortzufahren.

Hochladen der Benutzer durch USB-Stick



1. Klicken Sie auf Export Benutzer zu USB.
2. Wählen Sie Benutzer entsprechend der Abteilung oder individuelle Benutzer
3. Klicken Sie zum Wählen das USB- Laufwerk mit dem angesteckten USB-Stick
4. Wählen Sie die Arten der hochzuladenden Benutzerinformationen.

   FP VX 9 –FP VX 9 -Benutzer; Fingerabdruck durch Algorithmus VX 9.0 (alte Fingerabdruckvorlage) eingelesen.

   FP VX 10 -Benutzer; Fingerabdruck durch Algorithmus VX 10.0 (neue Fingerabdruckvorlage) eingelesen.

   Gesicht - Gesichtsvorlage des Benutzers.

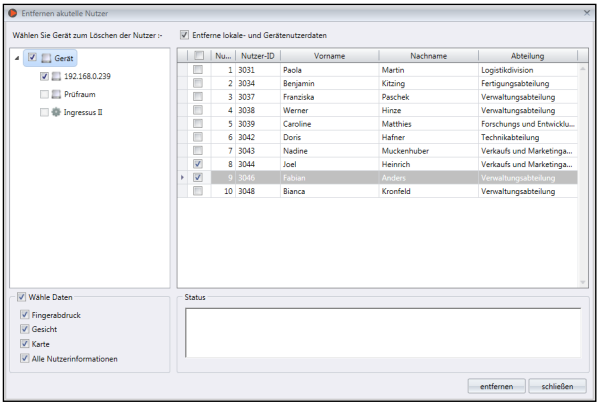
   Karte - Benutzer Kartennummer.
5. Wählen Sie Gerätearten, um die Daten zu laden
6. Klicken Sie auf Export.

Benutzer entfernen

Wenn die Benutzer nicht mehr in der Umgebung arbeiten oder sie nicht in eine andere Abteilung/Sektion übertragen werden können, müssen Sie deren Informationen von Ingress und aus den Geräten löschen. Hiermit stellen Sie sicher, dass der Benutzer keinen Zugriff mehr auf ausgewählte Türen hat.

Aktuelle Benutzer entfernen

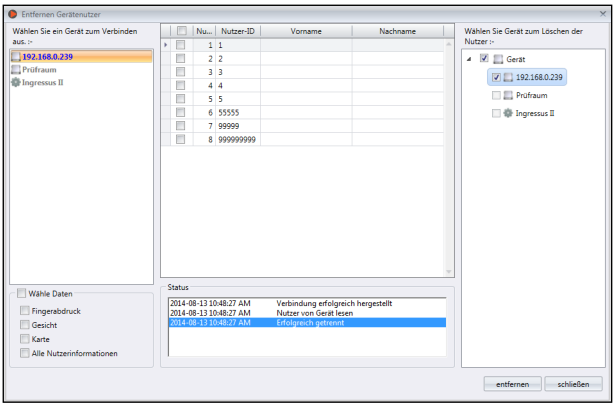
So können Sie Nutzer entfernen, die nicht mehr im Unternehmen arbeiten. Dieser Prozess kann die Information des Benutzers von Ingress und von allen Geräten entfernen.



1. Klicken Sie auf Aktuelle Benutzer Entfernen.
2. Wählen sie die Geräte aus dem linken Feld, um die Benutzer zu entfernen (empfohlen, alle auszuwählen)
3. Wählen Sie alle Daten löschen (Fingerabdruck, Gesicht, Karte, alle Benutzer-Info).
4. Wählen Sie die zu löschende Benutzer-ID.
5. Klicken Sie auf Entfernen, um fortzufahren.

Entfernen von Terminal- Benutzern

So können Sie Nutzer von ausgewählten Geräten entfernen. Die Information des Benutzers werden noch in Ingress behalten und können in Zukunft wieder auf Geräte übertragen werden.

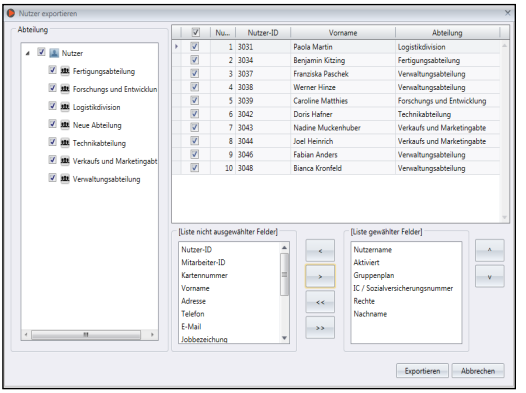


1. Klicken Sie auf Entfernen Sie die Benutzer des Gerätes.
2. Wählen Sie das Gerät (aus dem linken Feld),um es zu verbinden, sodass Sie die Benutzer-ID finden können, um sie zu löschen.
3. Wählen Sie die Benutzer-ID aus, um sie zu löschen.
4. Wählen Sie das Gerät (aus dem rechten Feld), um es zu verbinden, sodass Sie die Benutzer aus diesem Gerät löschen können.
5. Klicken Sie auf Entfernen, um fortzufahren.

Weitere Operation

Um die Personaldaten des Benutzers zu exportieren

Sie können die Personaldaten des Benutzers in andere digitale Formate (TXT, XLS, XLSX-oder CSV) oder in andere Systeme exportieren, um sie dort zu verwenden.



1. Klicken Sie auf Export-Benutzer.
2. Wählen Sie die Benutzer nach der Abteilung oder einzelne Benutzer.
3. Wählen Sie die Art der Personaldaten, die exportiert werden soll.
4. Drücken Sie den rechten Pfeil, um die Daten in de Exportprozess einzufügen.
5. Klicken Sie auf Export, um fortzufahren.
6. Benennen Sie die Ausgabedatei.
7. Wählen Sie die Art der Ausgabe aus.

Um die Benutzer durch Schlaglwörter zu suchen

Sie können die Ingress -Datenbank nach Benutzern durch Schlagwörter (Suchbegriffe), wie folgt durchsuchen:

1. Klicken Sie auf Benutzer suchen.
2. Geben Sie Schlagwörter in die entsprechende Spalte ein.
3. Klicken Sie auf Suche, um fortzufahren

Kapitel 5

Zugriffsebenen

Dieses Kapitel zeigt Ihnen, wie Sie den Benutzern zugeordnete Zugangsberechtigungen am Arbeitsplatz durch verschiedene Methoden erstellen können und hierduch Zugänge beschränken können:

Sie können den Zugriff für jede Benutzer nach Zeitraum zu jeder Tür am Arbeitsplatz beschränken, indem Sie entsprechende Einstellungen konfigurieren und auf die Geräte hochladen. Die terminals erlauben den Zugang, indem Sie die Identität des Benutzers und den vorgegebenen Zeitraum überprüfen. Zum Beispiel, können Sie den Zugriff für alle Führungskräfte zu allen Zeiten ermöglichen, aber können den Zugriff für andere Mitarbeiter auf 9:00 Uhr bis 17:00 Uhr beschränken.

Jeder Zeitraum ist in drei Zeitintervalle eines Tag gesplittet. Sie können in maximal drei Zeiträumen die Zutrittszeit eines Tag festlegen. Die Benutzer können den Arbeitsplatz nur während dieser drei Intervalle betreten. Zum Beispiel, können Sie den Zutritt für die Produktionsarbeiter in den Produktionsbereich von 7:00 Uhr bis 10:00 Uhr, von 11:00 Uhr bis 13:00 Uhr und von 14:00 bis 18:00 Uhr erlauben, damit sie ihrer Arbeit nachgehen können. Während der Pausen zwischen diesen 3 Zeiträumen haben die Produktionsarbeiter keinen Zugang in die Fabrik.

Sie können auch spezifische Zugangszeiten einstellen und auf den Urlaub anwenden. Ingress lädt die Zugriffszeit zusammen mit den Urlaubszeiten auf Geräte. Zum Beispiel können Sie den Zugang durch den Haupteingang nur von 8.00 Uhr bis 00:00 Uhr während der Ferien ermöglichen. Um die Urlaubseinstellungen vollständig nutzen zu können, müssen Sie die Liste der gültigen Feiertage bei Ingress einstellen, bevor weitere Konfigurationen durchgeführt werden.

Sie können die Sicherheit des Zugangs verbessern, indem Sie eine Kombination der Verifikationsmethoden benutzen. Um dies zu tun, können Sie verschiedene Verifikationsmethoden an einzelnen Türen einstellen. Zum Beispiel, F&E-Personal muss sich mit dem Fingerabdruck am Haupteingang des Unternehmens verifizieren, aber sie müssen sich zwingend sowohl mit Fingerabdruck als auch mit Karte verifizieren, wenn sie in das F & E-Büro gehen.

Zugriffsebene nach Zeit

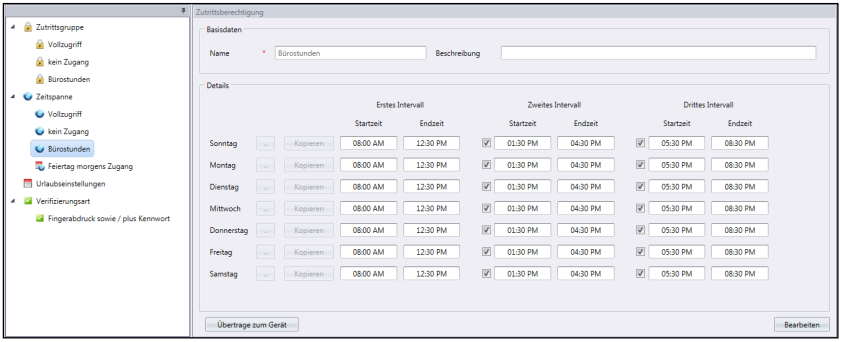
Zunächst müssen Sie die tägliche Zeiteinstellung konfigurieren. Eingestellte Zeit ist die Zeit, in der den Benutzern der Zugang in die Türerlaubt ist. Das Terminal verwehrt den Benutzerzugriff außerhalb dieser Zeit. Sie können bis zu 3 verschiedenen Zeiträumen an einem Tag einstellen.

Als nächstes müssen Sie Zugangsgruppen erstellen, und Zeiträume und Geräte definieren, die auf diese Gruppe angewendet werden.

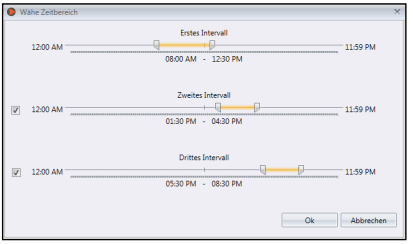
Schließlich, müssen Sie die Benutzer in die Zugangsgruppe hinzufügen. Die Benutzer müssen den Zeiteinstellungen der einzelnen Geräte folgen, um den Zugang zu erhalten.

Einstellung des Zeitraums

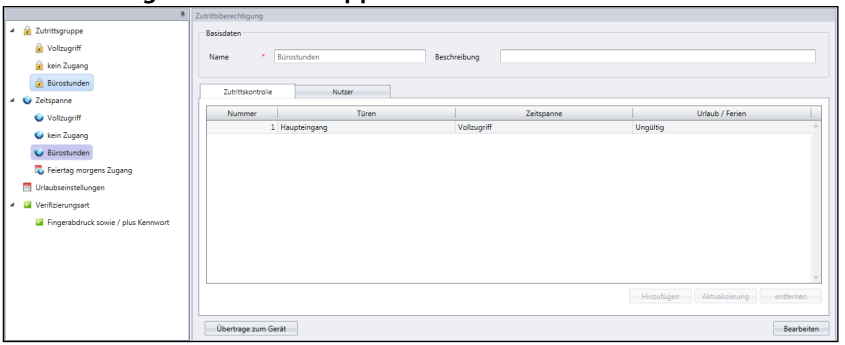
Standardmäßig bietet Ingress 2 Zeiträume, Jederzeit (immer zugreifbar) und Keinerzeit (nie zugreifbar). Sie können einen neuen Zeitraum nach den Anforderungen Ihres Unternehmens erstellen.

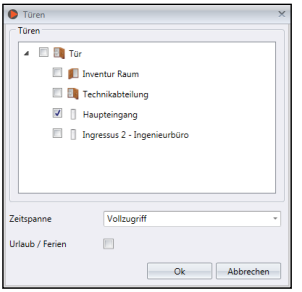


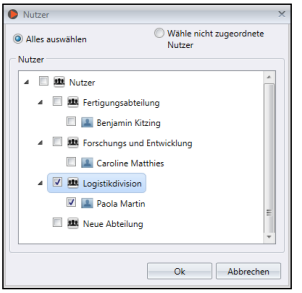
1. Wählen Sie Zeiteinstellung aus dem linken Feld.
2. Klicken Sie auf Zeit hinzufügen.
3. Drücken Sie auf Bearbeiten.
4. Benennen Sie den Zeitraum, z.B. Bürozeiten.
5. Schreiben Sie eine Beschreibung, um den Zeitraum zu bezeichnen.
6. Stellen Sie den Zeitbereich ein, um den Zugang mit maximalen 3 Zeitspannen pro Tag zu ermöglichen. Wollen Sie den Zugang für den ganzen Tag blockieren, Stellen Sie 23:59 Uhr als Anfangszeit und 24:00 Uhr als Endzeit ein.
7. Sie können Sie auf ... klicken, um alternativ grafische Einstellungen zu verwenden.
8. Um das zweite und das dritte Intervallzu verwenden, müssen Sie das Kontrollkästchen ankreuzen, um es zu aktivieren.
9. Klicken Sie auf Kopieren in der nächsten Zeile, wenn Sie die gleiche Zeit aus den oben genannten Einstellungen mehrfach anwenden möchten.
10. Klicken Sie auf Speichern, um die Einstellungen zu speichern.
11. Klicken Sie auf Übertragen auf das Gerät, um die Einstellungen mit dem Geräten zu synchronisieren.



Einrichtung der Zutritts-Gruppe





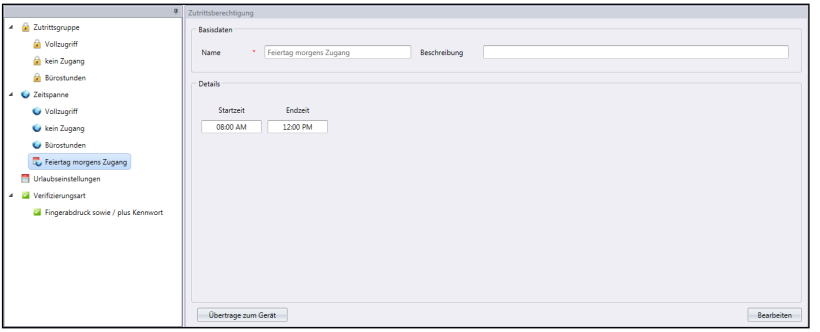


1. Klicken Sie auf Zutrittsgruppe im linken Feld.
2. Klicken Sie auf Zutrittsgruppe hinzufügen.
3. Bennen Sie die Zutrittsgruppe, z.B. Leitungsebene.
4. Klicken Sie auf Bearbeiten in der Zutrittskontrolltabelle.
5. Klicken Sie auf Hinzufügen, um das Gerät hinzufügen, um das Zutritts-Level zu verwenden.
6. Wählen Sie Zeiteinstellung aus, um diese anzuwenden (die Zeiteinstellung muss vor diesem Schritt voreingestellt sein).
7. Kreuzen Sie Ferien an, wenn Sie Ferienzeitzonen anwenden wollen(siehe *Kapitel 5 • Zutrittsebene in Ferien* für weitere Details).
8. Klicken Sie auf OK, um die Einstellungen zu speichern.
9. Klicken Sie auf Übertragen auf das Gerät, um Einstellungen mit dem Gerät zu synchronisieren.
10. Klicken Sie auf Bearbeiten in der Benutzertabelle.
11. Klicken Sie auf Hinzufügen, um die Benutzer einzufügen, die dieser Zutrittsgruppe und Zeiteinstellung folgen werden.
12. Klicken Sie auf OK, um die Einstellungen zu speichern.
13. Klicken Sie auf Übertragen auf das Gerät, um die Benutzer mit dem Gerät zu synchronisieren, die dieser Zutritts-Gruppe folgen werden.

Zutrittsebenen in den Ferien

Sie können den Zugriff von Benutzern während der Ferien steuern, z.B. die Benutzer können während der Ferien nur durch den Haupteingang des Unternehmens von 9:00 Uhr bis 00:00 Uhr eintreten. Richten Sie den Urlaubszeitraum ein, um die Zugriffszeit bei Ingress zu definieren, die auf den Urlaub anwendbar ist. Ingress ermöglicht es Ihnen nicht, fortzufahren, wenn Sie keinen Urlaubszeitraum definiert haben. Definieren Sie das Anfangs-und Enddatum für die Ferien unter Urlaubseinstellungen. Weisen Sie den Urlaubszeitraum auf einen bestimmten Urlaubs zu, um wirksam zu werden.

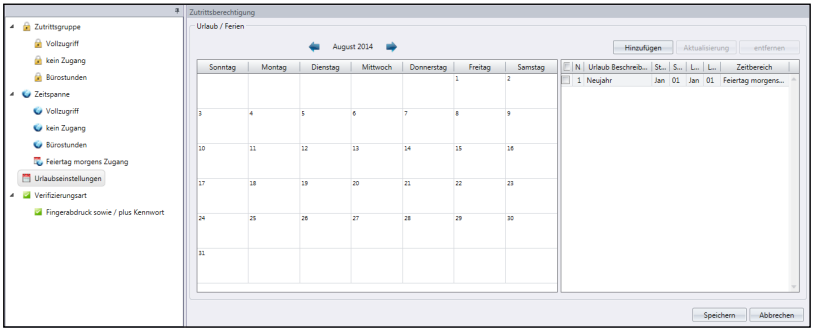
Einrichtung der Ferienzeiteinstellung



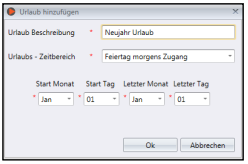
1. Klicken Sie auf Zeiteinstellung im linken Feld.
2. Klicken Sie auf fügen Sie Ferienzeitraum hinzu.
3. Beschreiben Sie den Urlaubszeitraum, z.B. Weihnachtsurlaub.
4. Klicken Sie auf Bearbeiten.
5. Bennen Sie den Urlaubszeitraum, z.B. Ferienzugang - Vormittags.
6. Definieren Sie die Anfangs-und Endzeit, für den Zugang.
7. Klicken Sie auf Speichern, um die Einstellungen zu speichern.
8. Klicken Sie auf Übertragen zum Gerät.

Sie können die oben genannten Schritte wiederholen, um zusätzliche Urlaubszeiten zu erstellen, die zum Arbeitsplatz passen.

Erstellen Sie die Ferienliste, um sie den Urlaubszeiteinstellungen hinzuzufügen

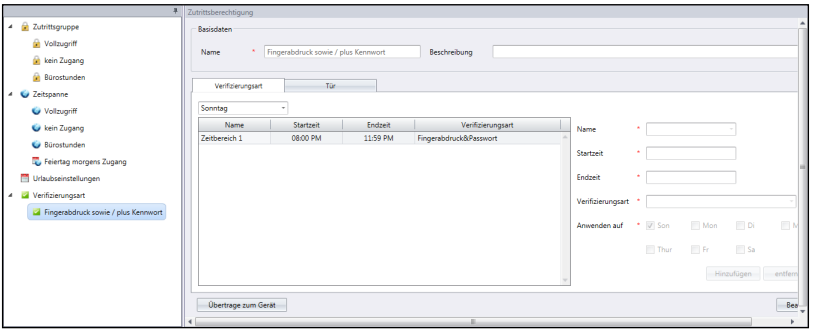


1. Klicken Sie auf Ferien Einstellungen im linken Feld.
2. Klicken Sie auf Bearbeiten.
3. Klicken Sie auf Hinzufügen, um neue Ferien hinzuzufügen.
4. Benennen Sie die Ferien.
5. Wählen Sie Ferienzeitzone aus, um zu bestätigen.
6. Definieren Sie das Anfangs-und Enddatum.
7. Klicken Sie auf OK, zur Bestätigung
8. Klicken Sie auf Speichern, um die Einstellungen zu speichern.
9. Klicken Sie auf übertragen auf das Gerät, um mit den Geräten zu synchronisieren.



Zutrittseben durch Verifizierungstyp

Sie können die Sicherheitsstufe des Zugangs durch die Anwendung verschiedener Verifikationsarten (Kombination der Prüfung) zu verschiedenen Zeiten erhöhen. Mit dieser Einstellung, müssen die Benutzer während einen bestimmtes Zeitraumes mehrere Verifizierungen am Gerät durchführen, um Zugang zu erhalten.



1. Klicken Sie auf Verifikationsstyp in dem linken Feld.
2. Klicken Sie auf fügen Sie den Verifikationstyp hinzu.
3. Bezeichnen Sie den Verifizierungstyp, zum Beispiel, FP + Passwort.
4. Wählen Sie Bennen aus (Sie können aus dem Zeitraum 1 bis 50 auswählen).
5. Definieren Sie die Anfangs-und Endzeit, die für diese Verifizierungsmethode anwendbar ist.
6. Wählen Sie Verifizierungstyp aus.
7. Klicken Sie auf Hinzufügen.
8. Wiederholen Sie die obigen Schritte, wenn Sie neue Verifizierungstypen in die Gruppe hinzufügen möchten.
9. Klicken Sie auf Speichern, um die Einstellungen zu speichern.
10. Klicken Sie auf Übertragen auf das Gerät, um die Einstellungen mit den Terminals zu synchronisieren.
11. Klicken Sie auf die Tür Tabelle.
12. Klicken Sie auf Hinzufügen, um die Türen auszuwählen, die für diese Verifizierungsmethode anwendbar sind.
13. Klicken Sie auf Speichern, um die Einstellungen zu speichern.
14. Klicken Sie auf Übertragen auf das Gerät, um die Einstellungen mit dem Gerät zu synchronisieren.

Kapitel 6

Überwachung

Dieses Kapitel zeigt Ihnen mehrere Methoden, um die Tür-Aktivitäten mit Ingress zu überwachen.

Die Überwachung der Tür-Aktivitäten ist bei einer Zutrittskontrollsoftware einer der zentralen Punkte. Die Geräte benötigen eine TCP/IP oder RS485 Verbindung, um außergewöhnliche Tür-Aktivitäten sofort an Ingress zu senden. Es ist sehr wichtig, die Netzwerkverbindung zwischen Ingress und allen Geräten abzusichern. Ebenso müssen die Tür-Sensoren installiert werden und mit allen Geräten verbunden werden. Der Tür-Sensor ist ein Magnetschalter, der als "Wächter" jeder Tür dient. Die Überwachung funktioniert nicht ohne einen an Tür und Terminal installierten Tür-Sensor.

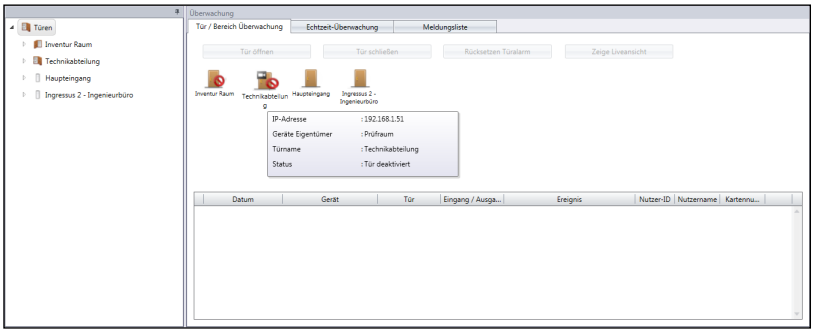
Ingress bietet 2 verschiedene Überwachungsmethoden. Sie können entweder die Aktivitäten jeder Tür überwachen oder durch eine visuelle Gebäudekarte . Es wird empfohlen, den Gebäudeplan Ihres Arbeitsplatzes bei Ingress als visuelle Karte zu importieren. Sie können für eine einfache Überwachung jede Tür auf die visuellen Karte ziehen und ablegen.

Sie können die Ereignisarten anpassen, die in Ingress gezeigt werden sollen. Es gibt insgesamt 48 Ereignisarten für Ingressus und 14 Ereignisarten für Standalone-Geräte. Alle außergewöhnlichen Vorfälle, die an Ingress gemeldet wurden, werden auf dem Bildschirm in verschiedenen Farben gezeigt. Sie können auch akustische Signale in Ingress aktivieren um Sie zu warnen, wenn ungewöhnliche Aktivitäten festgestellt werden.

Ingress kann auch unmittelbar E-Mails an definierte Benutzer senden,um außergewöhnliche Aktivitäten zu melden. Konfigurieren Sie die SMTP-E-Mail-Server-Einstellungen, damit Ingress erlaubt wird, Benachrichtigungs-Mails zu senden.

Darüber hinaus, können Sie in den Überwachungsprozess IP-Kameras (Milestone oder EpiCamera) integrieren. Ingress kann das Material von Ihrer Videoüberwachungssoftware zurückzuspielen, um Ihnen die gewünschte Szene zu zeigen.

Überwachung von Tür oder Zone

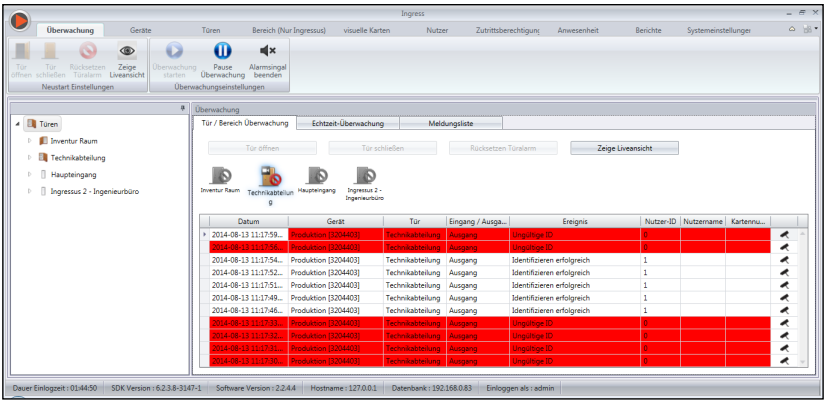


Öffnen Sie die Überwachung Registerkarte, um alle Türen anzuschauen, die auf dem Bildschirm angezeigt werden. Ingress zeigt die Details einer Tür, wenn Sie den Mauszeiger darauf ziehen. Klicken Sie auf die Tür-Gruppe im linken Feld, um die Türen zu sehen , die in dieser Tür-Gruppe zugeordnet sind.

Jedes Tür-Symbol stellt den aktuellen Zustand der Türen dar. Sehen Sie die Details unten:

Tür-Symbol	Bedeutung
	Die Geräte sind mit der Tür gekoppelt und arbeiten online. Alles ist normal.
	Die Verbindung mit den Geräten dieser Tür ist unterbrochen. Erfordert sofortiges Handeln, um die Geräte zu überprüfen.
	Es wurden keine Geräte mit dieser Tür verbunden. Stellen Sie sicher, dass Sie die Geräte zur Liste hinzugefügt haben und fügen Sie die Geräte zur Tür hinzu.
	Tür ist mit eingebauter IP-Kamera. Sie können Live-Ansicht anschauen, um diese Tür zu überwachen.
	Türalarmauslösung durch gewaltsames Öffnen der Tür oder Tür nicht verschlossen. Erfordert sofortiges Handeln, um die Tür zu überprüfen.

Der untere Teil des Bildschirms stellt alle Aktivitäten, die von allen Geräten gesendet wurden, dar. Sie können IN-OUT-Datensätze aller Benutzer, Türaktivitäten und Alarmauslöser ansehen.



Fern-Einstellungen

Sie können alle Türen per Fernbedienung durch Ingress steuern. Sie können das Öffnen / Schließen der Türen steuern oder den Türalarm zurücksetzen.

Um die Tür automatisch zu öffnen/schließen:

1. Wählen Sie dieTür aus Tür / Zone-Überwachung aus.
2. Klicken Sie auf dieTür öffnen oder die Tür schließen.

Hinweis: *Klicken Sie auf Tür-Schließen, damit der Terminal oder Ingressus das Türschloss-System sofort verriegelt.*

Um den Türalarm zurückzusetzen:

1. Wählen Sie dieTür aus Tür / Zone-Überwachung aus.
2. Klicken Sie auf das Zurücksetzen des Türalarms.

Hinweis: *Zas Zurücksetzen des Türalarms funktioniert nur, wenn der Tür-Alarm aktiviert wird.*

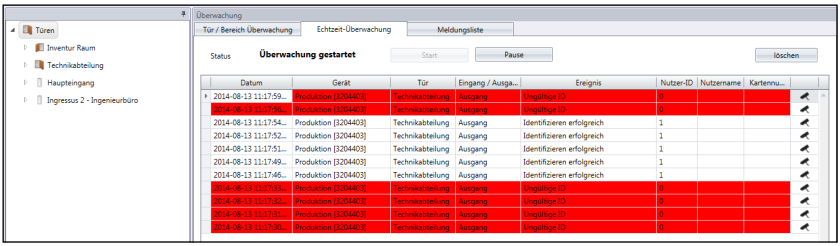
Überwachungseinstellungen

Ingress startet den Überwachungsprozesse automatisch, wenn Sie diese Seite öffnen. Sie können den Prozess anhalten, indem Sie auf die Pause-Überwachung -Taste drücken.

Ingress löst Ihren Lautsprecher am PC oder Laptop aus, um Sie im Falle der außergewöhnlichen Aktivitäten zu warnen. Sie können auf die Alarmton anhalten -Taste drücken, um die Alarmmeldung zu bestätigen.

Echtzeit-Überwachung

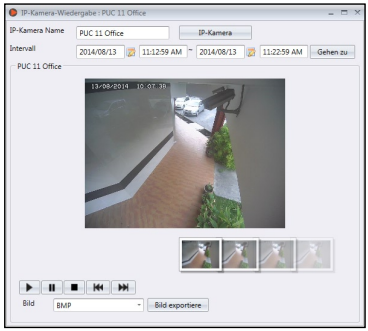
Die Echtzeit-Überwachung Seite zeigt alle Datensätze aus allen Geräten. Sie können jeden Datensatz zeilenweise ansehen. Sie können den Vorgang anhalten, wenn Sie sich auf bestimmte Datensätze konzentrieren wollen. Klicken Sie auf Start-Taste, um den Vorgang fortzusetzen.


Überwachung
Türen
Inventur Raum
Technikabteilung
Haupteingang
Ingressus 2 - Ingenieurbüro
Tür / Bereich Überwachung
Echtzeit-Überwachung
Meldungsliste
Status
Überwachung gestartet
Start
Pause
löschen
Datum
Gerät
Tür
Eingang / Ausga...
Ereignis
Nutzer-ID
Nutzername
Kartennu...
2014-08-13 11:17:59... Produktion [3204403] Technikabteilung Ausgang Ungültige ID 0
2014-08-13 11:17:56... Produktion [3204403] Technikabteilung Ausgang Ungültige ID 0
2014-08-13 11:17:54... Produktion [3204403] Technikabteilung Ausgang Identifizieren erfolgreich 1
2014-08-13 11:17:52... Produktion [3204403] Technikabteilung Ausgang Identifizieren erfolgreich 1
2014-08-13 11:17:51... Produktion [3204403] Technikabteilung Ausgang Identifizieren erfolgreich 1
2014-08-13 11:17:49... Produktion [3204403] Technikabteilung Ausgang Identifizieren erfolgreich 1
2014-08-13 11:17:46... Produktion [3204403] Technikabteilung Ausgang Identifizieren erfolgreich 1
2014-08-13 11:17:33... Produktion [3204403] Technikabteilung Ausgang Ungültige ID 0
2014-08-13 11:17:32... Produktion [3204403] Technikabteilung Ausgang Ungültige ID 0
2014-08-13 11:17:31... Produktion [3204403] Technikabteilung Ausgang Ungültige ID 0
2014-08-13 11:17:30... Produktion [3204403] Technikabteilung Ausgang Ungültige ID 0

Sie werden an einigen Datensätzen ein kamerasymbol sehen. Dies zeigt, dass die Tür mit einer IP-Kamera verbunden ist. Doppelklicken Sie auf den Bericht, um Live-Aufnahmen durch die IP-Kamera zu sehen.

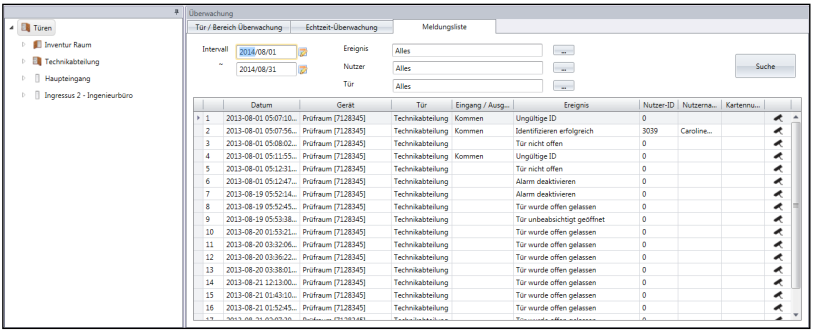
Wenn Türalarm ausgelöst wird, markiert Ingress den Bericht rot, um Sie zu warnen. Doppelklick auf den Bericht und Ingress wird das Videomaterial aus der Videoüberwachungssoftware für Ihre Referenz streamen.

Ingress ruft das Video immer 5 Minuten vor und nach der Türalarmauslösung ab. Sie können die Bilder in digitale Formate (BMP, JPEG, PNG, GIF, TIFF) exportieren. Sie können sie auch in AVI oder MKV-Videoformate exportieren.



Zutrittsprotokoll

Um bei Ingress nach vorherigen IN-OUT Datensätzen oder nach den Alarm-Datensätzen zu suchen, können Sie in der Registerkarte Zutrittsprotokolle nachschauen.

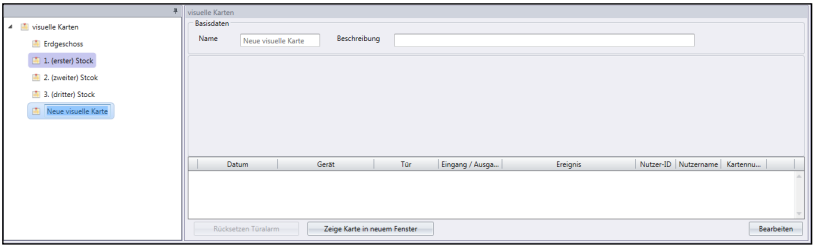

Türen
Inventur Raum
Technikabteilung
Haupteingang
Ingressus 2 - Ingenieurbüro
Überwachung
Tür / Bereich Überwachung
Echtzeit-Überwachung
Meldungsliste
Intervall
2014/08/01
2014/08/31
Ereignis
Alles
Nutzer
Alles
Tür
Alles
Suche
Datum
Gerät
Tür
Eingang / Ausg...
Ereignis
Nutzer-ID
Nutzerna...
Kartennu...
1 2013-08-01 05:07:10... Prüfraum [7128345] Technikabteilung Kommen Ungültige ID 0
2 2013-08-01 05:07:56... Prüfraum [7128345] Technikabteilung Kommen Identifizieren erfolgreich 3039 Caroline...
3 2013-08-01 05:08:02... Prüfraum [7128345] Technikabteilung Tür nicht offen 0
4 2013-08-01 05:11:55... Prüfraum [7128345] Technikabteilung Kommen Ungültige ID 0
5 2013-08-01 05:12:31... Prüfraum [7128345] Technikabteilung Tür nicht offen 0
6 2013-08-01 05:12:47... Prüfraum [7128345] Technikabteilung Alarm deaktivieren 0
7 2013-08-19 05:52:14... Prüfraum [7128345] Technikabteilung Alarm deaktivieren 0
8 2013-08-19 05:52:45... Prüfraum [7128345] Technikabteilung Tür wurde offen gelassen 0
9 2013-08-19 05:53:38... Prüfraum [7128345] Technikabteilung Tür unbeabsichtigt geöffnet 0
10 2013-08-20 01:53:21... Prüfraum [7128345] Technikabteilung Tür wurde offen gelassen 0
11 2013-08-20 03:32:06... Prüfraum [7128345] Technikabteilung Tür wurde offen gelassen 0
12 2013-08-20 03:36:22... Prüfraum [7128345] Technikabteilung Tür wurde offen gelassen 0
13 2013-08-20 03:38:01... Prüfraum [7128345] Technikabteilung Tür wurde offen gelassen 0
14 2013-08-21 12:13:00... Prüfraum [7128345] Technikabteilung Tür wurde offen gelassen 0
15 2013-08-21 01:43:10... Prüfraum [7128345] Technikabteilung Tür wurde offen gelassen 0
16 2013-08-21 01:52:45... Prüfraum [7128345] Technikabteilung Tür wurde offen gelassen 0

1. Definieren Sie die Anfangs- und End Zeit, um die Datensätze zu suchen.
2. Wählen Sie die Art von Datensätzen aus, die Sie benötigen (Ereignis, Benutzer oder Gerät).
3. Spezifische Art der Veranstaltung, Benutzer-ID oder Geräte-ID.
4. Klicken Sie auf Suche.

Visuelle Karte

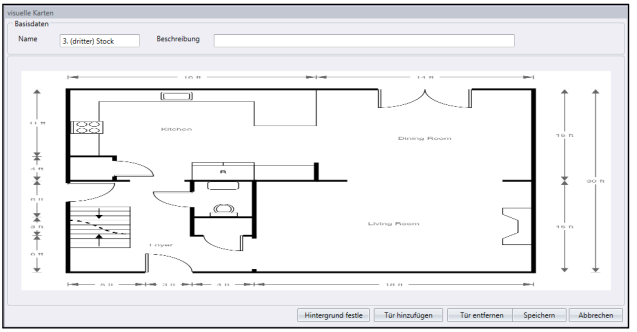
Sie können Grundrisse (im JPEG-Format) in Ingress importieren, um sie als visuelle Karte zu verwenden. Sie können die Türen ziehen in die Karte für einen vollständige Überblich bei der Überwachung ablegen. Im Falle einer ungewöhlichen Tür-Aktivität, wird die Tür zusammen mit einem Warnton auf Ihrem PC blinken. Sie können den Tür-Alarm zurückzusetzen, wie *in Kapitel 6 angezeigt worden ist • Remote-Einstellungen*. Sie können jede Tür öffnen / schließen, indem Sie die Tür aus der Karte ausgewählen, und indem Sie auf die Tür öffnen oder die Tür schließen -Tasten drücken.

Einfügen von visueller Karte und Türen



1. Klicken Sie auf Visual Map im linken Fenster.
2. Klicken Sie auf Visual Map hinzufügen um ein neuen Gebäudeplan zu erstellen.
3. Name des Gebäudeplans, z.b.: 3. Stockwerk.
4. Drücken Sie auf Bearbeiten um Konfigurieren zu starten.

Richten Sie den Hintergrund ein - Um den Grundriss auszuwählen, der als visuelle Karte verwendet werden soll.
Fügen Sie die Tür ein - Wählen Sie die Tür aus, die in die visuelle Karte hinzugefügt werden soll. Ziehen Sie die Tür an die richtige Stelle auf der Karte.



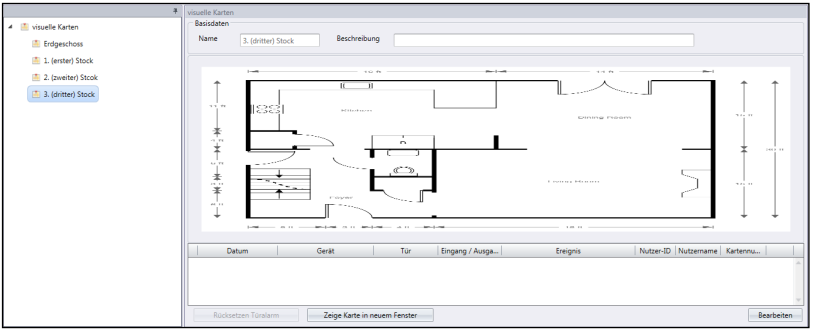
Entfernen Sie die Tür - Wählen Sie das Tür-Symbol aus der Karte aus und klicken Sie auf Entfernen Sie die Tür, wenn die Tür nicht mehr im Gebrauch ist.

5. Klicken Sie auf Speichern um die Einstellungen zu speichern.

Starten des Überwachungsvorgangs

Sie können den Überwachungsprozess starten, indem Sie obnen im Menue auf Überwachung starten drücken. Klicken Sie auf [Pause- Überwachung], wenn Sie den Vorgang stoppen wollen.

Klicken Sie auf Visuelle Karte im linken Fenster und Ingress wird alle Karten im rechten Fenster anzeigen. Klicken Sie auf die gewünschte visuelle Karte, wenn Sie eine Detailansicht der Karte sehen möchten.



Click Show Map in New Window and Ingress will display the selected map in an individual window. You can drag the individual map to another display monitor/LCD for all-time monitoring.

Kapitel 7

Zeiterfassung

Dieses Kapitel zeigt Ihnen die Einrichtung der Zeittafeln zur Aufzeichnung und Überwachung der Anwesenheit und erzeugt eine Anwesenheitsliste.

Ingress bietet eine umfangreiche Zeit- und Anwesenheitserfassung zur Anwendung bei nahezu allen Anforderungen unterschiedlicher Branchen. Um die Funktionen zu verwenden, müssen Sie zunächst die Zeittafeln festlegen. Die Zeittafeln bestehen aus der Wochenarbeitszeittabelle, den Berechnungsregeln für die Arbeitszeit und Überstunden. Die Benutzer an allen Geräten angemeldet werden, die am Arbeitsplatz installiert sind. Ingress lädet die Aufzeichnungen von Geräten herunter und führt die Anwesenheitsliste entsprechend der Zeittafeln. Sie können bis zu 999 verschiedene Zeitpläne in die Software einstellen.

3 wichtige Arten von Zeittafeln können übersichtlich in Ingress verwendet werden

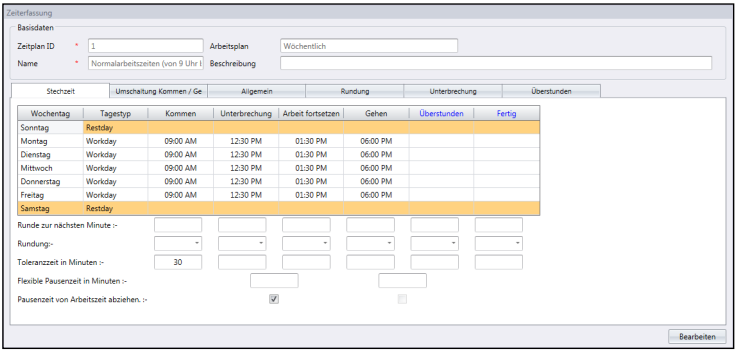
- WÖCHENTLICH - Wöchentlich rotierende Zeittafeln
  Dieser Zeitplan ist der am häufigsten verwendete Arbeitsplan weltweit, bei den Arbeitstage mit Wochentagen übereinstimmen.
- TÄGLICH - Täglich rotierende Zeittafeln
  Dieser Zeitplan ist optimal für den Mehrschichtbetrieb, bei denen sich Arbeitszeiten täglich ändern.
- FLEXIBEL - Geeignet für Arbeitnehmer mit flexiblen Arbeitszeiten.

Die nächste wichtige Konfiguration ist der Gruppendienstplan oder Jahresarbeitskalender. Sie können die Benutzer in eine einzige Gruppe einteilen, wenn sie deie gleichen Arbeitsbedingungen haben oder Sie passen unabhängige Kalender auf bestimmte Benutzer unter Nutzerarbeitszeitplan an. Jeder Gruppendienstplan folgt einer Zeittafel. Ingress bietet insgesamt 999 Gruppendienstpläne zur Verwendung an.

Sie können verschiedene Abwesenheitsarten zu Ingress hinzufügen. Die Abwesenheiten werden im Anwesenheitsplan aufgenommen. Eine Spalte für Bemerkungen ist verfügbar, um die ungewöhnliche Abwesenheiten zu markieren. Die Benutzer können Kurbezeichnungen bei der Verifizierung einfügen, wobei jede Kurzbezeichnung einen Sachverhalt beschreibt, um die außergewöhnliche Abwesenheit zu erklären.

Wöchentliche Zeittafeln

Taktungsregeln



Die Zeitnahme erfordert eine Aktivität des Mitarbeiters am jeweiligen Zeitnahmegerät. Ingress bietet 6 Anwesenheitsspalten in 3 Paaren an.

1. Klicken Sie auf Zeittafel im linken Fenster.
2. Klicken Sie auf Zeittafel Hinzufügen.
3. Bennen Sie den Dienstplan, z.B. Normale Arbeitszeit von 09:00 Uhr bis 18:00 Uhr.
4. Benennen Sie die Zeittafel, z. B. Normaler Arbeitstag 09:00 bis 18:00 Uhr.
5. Wählen sie wöchentlich unter Zeittafel.
6. Benennen Sie die Zeittafel.
7. Klicken Sie auf OK.

Kommen - Gehen	Dieses Paar ist sehr wichtig, es zeigt den ersten Datensatz eines Benutzers in der [kommen Spalte] und den letzten Datensatz in der gehen Spalte.
Pause Fortsetzen	Diese Spalte registriert den Anfang der ersten Pausenzeit in der Pausenspalte und die Endzeit der ersten Pause der Zusammenfassungsspalte. Diese Spalte ist nicht zwingend; Sie können diese verlassen, wenn Sie die Pausenzusammenfassung nicht ansehen möchten.

Geleistete Überstunden	Diese Spalte registriert die Anfangszeit der Überstunden in Überstunden und die Endzeit der Überstunden in geleistet. Diese Spalte ist nicht zwingend. Verlassen Sie diese Spalte, wenn Ihre Firma nicht verlangt, dass Mitarbeiter Überstunden zu gewissen Zeit beginnen oder beenden. Verlassen Sie diese Spalte, und Ingress wird die Überstunden automatisch berechnen, wenn ein Mitarbeiter nach der Standardarbeitszeit gestempelt hat. Im Falle dass Ihre Firma 2 Pausen pro Tag gewährt, können Sie dieEndzeit als Anfangszeit der zweiten Pause und Überstunden als die Endzeit der zweiten Pause behandeln. Auf diese Weise werden Überstunden nur berechnet, wenn ein Angestellter nach Standardzeit gestempelt hat.

8. Definieren Sie ein Standardzeit zur Auswertung

Erfahren Sie mehr über Zeitpaarungen in nachfolgender Tabelle.

1. Runden auf die nächste Minute - In jeder Zeitspalte können Sie gemäß Ihrer Firmenpolitik die Zeiten runden lassen. Erfahren Sie dazu mehr in nachfolgender Tabell.

   Aufrunden: Wenn Sie "aufrunden 15 Minuten" auswählen wird die Anmeldezeit auf volle 15 Minuten aufgerundet. Bei einer Anmeldung 09:06 Uhr wird automatisch auf 09:15 gerundet

   Abrunden: Wenn Sie "abrunden 15 Minuten" auswählen wird die Anmeldezeit auf volle 15 Minuten abgerundet. Bei einer Anmeldung 09:06 Uhr wird automatisch auf 09:00 gerundet.

   Mittelwert: Wenn Sie "Mittelwert" auswählen wird aus der Anmeldezeit ein Mittelwert gebildet. Bei einer Anmeldung 09:06 Uhr wird automatisch auf 09:07 gemittelt.

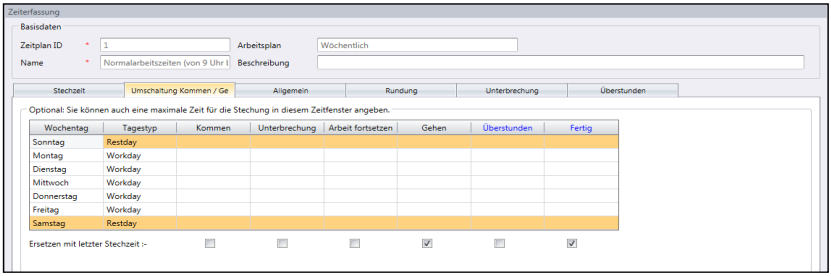
2. Erlauben Sie eine Toleranz in Minuten: Das hängt auch von Ihrer Unternehmenspolitik ab, ob es Mitarbeitern erlaubt ist zu früh oder zu spät zu kommen? Sie können die Dauer der Toleranz in Minuten in den gegebenen Spalten festlegen. Wenn Ihre Firma keine Toleranz zulässt, lassen Sie die Spalten einfach frei.

3. Flexible Pausenzeiten: Sie können Ihren Mitarbeitern erlauben Ihre Pausen in einer gewissen Zeitspanne zu erlauben. So ist es zum Beispiel erlaubt die Pausen in einem Zeitfenster von 12:30 Uhr bis 14:30 Uhr flexibel zu legen. Das Unternehmen kann auch die Pausenlänge bestimmen. Wenn zum Beispiel eine Pausendauer von einer Stunde definiert wird muss der Mitarbeiter spätestens nach der vorgegebenen Zeit die Pause beenden. Wird die Zeit überschritten wird Ingress dies vermerken. Wenn dies in Ihrem Unternehmen nicht anwendbar ist können Sie diese Eigenschaften ignorieren.

4. Ausschließen der Pausenzeit von der Arbeitszeit: Klicken Sie auf das Auswahlfeld, wenn Ihre Firma Pausenzeiten von der Gesamtarbeitszeit abzieht. Ignorieren Sie die Option, wenn es nicht relevant ist.

5. Klicken Sie auf OK, um die Einstellungen zu speichern.

Bereichsregeln

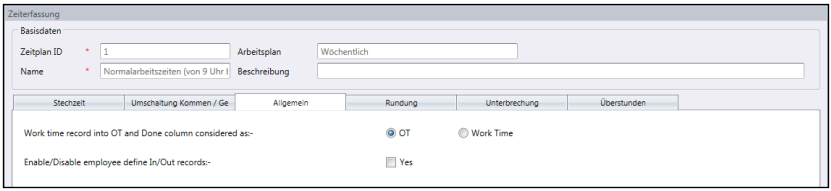


Wählen Sie diese Option um die maximale Zeit zu bestimmen die eine Spalte aufzeichnen kann bevor es in einer anderen spalte erfasst wird. Zum Beispiel wird einen kommen-Wert von 12:01 Uhr nicht mehr in der Spalte der Arbeitszeit erfasst sondern in den Pausenzeiten. Wenn Sie das Ende der Arbeitszeit mit 18:00 Uhr definieren wird jede angefangene Minute nach 18:00 Uhr in die Überstundenspalte einbezogen.

Ersetzen durch die letzte Zeitnahme –Wenn Sie auf dieses Kontrollkästchen klicken, wird Ingress die Zeitdaten durch die letzten Zeitdaten ersetzen, nachdem der Downloadprozess abgeschlossen ist. Es wird empfohlen, dass Sie dieses Kontrollkästchen für die Endzeiten auswählen, weil die Software immer die letzte Endzeit der Mitarbeiter überprüfen wird und sie auf der Zeittafel veröffentlicht.

1. Klicken Sie auf Taktbereich.
2. Klicken Sie auf Bearbeiten.
3. Konfigurieren Sie die Zeit in den Bereich Spalten.
4. Aktivieren Sie das Feld mit der neuesten Taktung Ersetzen für die Out-und Fertig-Spalten.

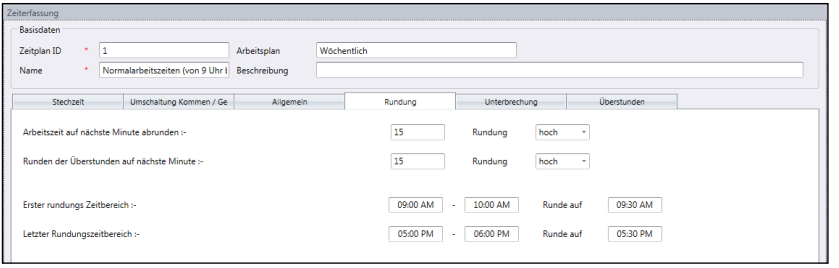
Generelle Regeln



Allgemein sollten Sie bestimmen welche Zeiten in die Überstunden mit einbezogen werden oder als normale Arbeitszeiten gelten. Klicken Sie auf den passenden Button um Ihre Wahl zu bestimmen. Wenn Sie die Zeiten als Überstunden definieren, wird die zusätzliche Zeit des Personals berechnet die diesen Zeitplan verwenden.

Sie können bestimmen das ein Mitarbeiter einen Knopf drücken muss um seine Arbeitszeit einzugeben.

Rundungsregeln



Das Runden soll das “Runden von Minuten” in der Zeitplanung und die Darstellung der Zeittafeln festlegen.

Erfahren Sie mehr ich der nachfolgenden Tabelle:

Runden Sie die Arbeitszeit (Minuten)

Aufrunden	Die Arbeitszeit wird im 15 Minuten-Takt aufgerundet: 1-15 Minuten = 15 16-30 Minuten = 30 31-45 Minuten = 45 46-59 Minuten = 1 hour
Abrunden	Die Arbeitszeit wird im 15 Minuten-Takt abgerundet: 1-15 Minuten = 0 16-30 Minuten = 15 31-45 Minuten = 30 46-59 Minuten = 45
Mittelwert	Sobald Sie hier einen Wert einfügen, wird die Software den Mittelwert berechnen. Zum Beispiel, wenn Sie den Wert auf 15 Minuten setzen, würde der Mittelwert 7 Minuten betragen. Die Zeitplanung ist 9:00 Uhr, und der Mittelwert beträgt 7 Minuten. Wenn der Mitarbeiter sich in weniger als 7 Minuten nach Arbeitszeitbeginn verifiziert, zum Beispiel 9:07 Uhr, wird die Software die Transaktionsdaten nach abrunden. Wenn der Mitarbeiter sich erst nach mehr als 7 Minuten verifiziert, wird die Software auf 15 Minuten aufrunden(9:15 Uhr).

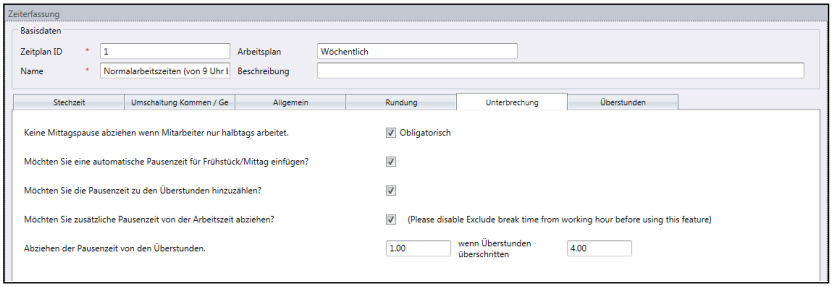
Auf- und Abrunden der Überstunden

Aufrunden	Überstunden werden im 15 Minuten-Takt aufgerundet: 1-15 Minuten = 15 16-30 Minuten = 30 31-45 Minuten = 45 46-59 Minuten = 1 hour
Abrunden	Überstunden werden im 15 Minuten-Takt abgerundet: 1-15 Minuten = 0 16-30 Minuten = 15 31-45 Minuten = 30 46-59 Minuten = 45
Mittelwert	Sobald Sie hier einen Wert einfügen, wird die Software den Mittelwert des Wertes berechnen. Zum Beispiel, wenn Sie den Wert in 30 Minuten einsetzen, würde der Mittelwert 15 Minuten sein. Die Überstundenzeit ist 18:00 Uhr, und der Mittelwert beträgt 15 Minuten. Wenn ein Mitarbeiter in weniger als 15 Minuten nach der eingestellten Überstundenzeit (z. B. 18:15 Uhr) auscheckt, wird die Software die Zeit abrunden (18:00 Uhr). Checkt er erst nach mehr als 15 Minuten aus wird die Software den Wert aufrunden (18:30 Uhr).

Erste gerundete Zeit - Diese Funktion wird nur für die kommen-Zeit angewendet. Sie könne diese Zeit nach Ihren Wünschen von der Software runden lassen. Zum Beispiel wird eine Transaktion zwischen 09:01 Uhr und 09:15 Uhr auf 09:00 Uhrt abgerundet

Letzte gerundete Zeit - Diese Funktion wird nur für die gehen-Zeit angewendet. Sie könne diese Zeit nach Ihren Wünschen von der Software runden lassen. Zum Beispiel wird eine Transaktion zwischen 17:01 Uhr und 17:15 Uhr auf 17:00 Uhrt abgerundet.

Pausenregeln

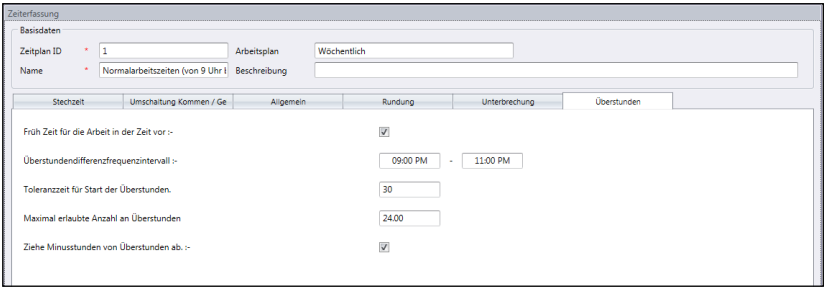


Pause soll die erlaubte Pausenzeit im Zeitplan bestimmen. Ausserdem bestimmen Sie wie die Pausen in der Zeittabellte angezeigt werden.

Erfahren Sie mehr über die Pausenregeln in nachfolgender Tabelle:

Keine Pausen abziehen wenn der Mitarbeiter nur halbtags beschäftigt ist.	Gibt es spezielle Regeln in Ihrer Firma klicken Sie bitte auf "Prüfen". Verlassen sie die Auswahl wenn dies für Ihre Firma nicht relevant ist.
Wollen Sie automatisch eine Pause hinzufügen zur Arbeitszeit hinzufügen?	Aktivieren Sie das Kontrollkästchen wenn die Pausenzeiten der Mitarbeiter die während den Pausen arbeiten zur Arbeitszeit hinzugefügt werden sollen.
Wollen Sie Pausen in die Überstunden einbeziehen?	Aktivieren Sie dieses Kontrollkästchen wenn Sie die nicht beendeten Pausenzeiten in die Überstunden einbeziehen wollen. Dies fügt Mitarbeitern Überstunden hinzu die während den Pausenzeiten gearbeitet haben.
Wollen Sie eine extra Pause von der Arbeitszeit abziehen?	Aktivieren Sie dieses Kontrollkästchen wenn Sie die Pausenzeit nach Ihren Vorgaben bechränken möchten. Überzieht der Mitarbeiter die Pausenzeit wird dies von den Gesamtarbeitsstunden abgezogen.
Deduct no. of hours for break time from overtime hour	Wenn Sie die Pausenzeit von den Überstunden abziehen definieren Sie eine Anzahl von Stunden die abgezogen werden sollten wenn die genommenen Überstunden einen bestimmten Wert überschreiten.

Überstundenregeln



Überstundenregeln werden im wöchentlichen Zeitplan bestimmt. Erfahren Sie mehr in nachfolgender Tabelle:

Zu früh beginnende Arbeitszeit	Manchmal beginnen Mitarbeiter zu früh mit ihren Überstunden. Wenn zum Beispiel die Überstundenregel erst ab 20:00 Uhr beginnt aber der Mitarbeiter schon 19:00 Uhr beginnt. Aktivieren Sie dieses Kontrollkästchen wenn Sie dies erlauben möchten.
Überstundendifferenzialzeit	Es gibt Überstundenregelungen die von einer Firma als Wenn-Basis gewährt werden. Definieren Sie kommen- und gehen-Zeit für diese Überstundenregelungen.

Minimale minutenanzahl zum erzeugen von Überstunden	Definieren Sie die Anzahl der Minuten, die mindestens gearbeitet werden müssen um sich für Überstunden zu qualifizieren.
Maximal erlaubte Anzahl von Überstunden	Setzen Sie ein Limit von Stunden die ein Mitabeiter für Überstunden beanspruchen kann. Das voreingestellte Maximum beträgt 24 Stunden.
Abziehen von Minusstunden von Überstunden	Wenn ein Angestellter an einem Arbeitstag nur kurz arbeitet werden die nicht gearbeiteten Stunden von den Überstunden abgezogen. Aktivieren Sie das Kontrollkästchen wenn Sie dies erlauben möchten.

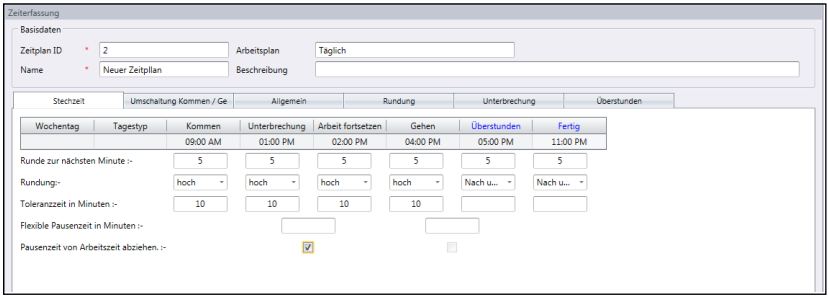
Tägliche Plantafel

Der tägliche Arbeitsplan ist nur verfügbar wenn Sie einen neuen Plan erstellen und auf "täglich" setzen. Der tägliche Zeitplan ist anwendbar für den Standardzeitplan.

Dieser ist geeignet für mehrfache Schichtenpläne, offene Schichtpläne oder Rotationspläne wo der Zeitplan sich täglich ändert. Es gibt 6 Registerkarten die Sie für tägliche Schichtpläne anlegen können.

1. Klicken Sie auf Zeittafel im linken Fenster.
2. Klicken Sie auf Zeittafel Hinzufügen.
3. Geben Sie die User-ID ein um die Zeittafel zuzuordnen.
4. Bennen Sie die Zeittafel.
5. Wählen Sie Täglich unter der Zeittafel.
6. Fügen Sie eine Beschreibung der Zeittafel ein.
7. Klicken Sie auf OK

Taktungsregeln



Die Zeiten beziehen sich auf die gestempelten Werte der Mitarbeitern an den Terminals. Ingress bietet Ihnen 6 Transaktionsspalten in 3 Paaren an. Sie können 6 Zeitpäne als tägliche

Zeittafeln setzen. Wenn Sie die Stechzeiten in den Zeitspalten definieren wird Ingress diese in die passenden Spalten legen.

Definieren Sie eine Standardzeit:

Kommen-Gehen	Dieses Paar ist sehr wichtig, es zeigt die ersten Daten der (Kommen Spalte) und den letzten Datensatz (kommen Spalte)
Pause machen	Diese Spalte registriert die Anfangszeit der Pause Pausenspalte und die Endzeit der ersten Pause. Die Spalte ist nicht zwingend und kann geschlossen werden wenn sie nicht benötigt wird.
Überstunden machen	Diese Spalte Überstunden registriert die Anfangszeit der Überstunden und die Endzeit Enzeit der Überstunden. Diese Spalte ist auch nicht zwingend. Lassen Sie diese Spalten, wenn Ihr Unternehmen erfordert keine Benutzer zu bestimmten Zeiten starten und beenden OT. Lassen Sie diese Spalte Blanks und Ingress automatisch Überstunden berechnen, wenn ein Mitarbeiter abgemeldet, nachdem der Standard Out Zeit. Im Falle das Ihr Unternehmen 2 Pausen am Tag berechnet können Sie die Endzeit als Beginn der zweiten Pausenzeit setzen. Auf diese Weise werden Überstunden erst nach der zweiten Pausenzeit berechnet.

1. Runden zur nächsten Minute - In jeder Zeitspalte könne Sie zur nächtsten Minute Runden lassen sollte dies in Ihrem Unternehmen so gehandhabt werden. Beziehen Sie sich auf nachfolgende Tabelle zum Runden der Zeiten.

   Aufrunden: Wenn Sie "aufrunden 15 Minuten" auswählen wird die Anmeldezeit auf volle 15 Minuten aufgerundet. Bei einer Anmeldung 09:06 Uhr wird automatisch auf 09:15 gerundet.

   Abrunden: Wenn Sie "abrunden 15 Minuten" auswählen wird die Anmeldezeit auf volle 15 Minuten abgerundet. Bei einer Anmeldung 09:06 Uhr wird automatisch auf 09:00 gerundet.

   Mittelwert: Wenn Sie "Mittelwert" auswählen wird aus der Anmeldezeit ein Mittelwert gebildet. Bei einer Anmeldung 09:06 Uhr wird automatisch auf 09:07 gemittelt.

2. Erlauben von Toleranzen - die hängt auch von Ihrer Firmenpolitik ab, ob Sie den Mitarbeitern gewisse Toleranzen in der Zeiterfassung erlauben. Sie können die Toleranzen in der Tabelle in jeder Spalte in Minuten festlegen. Wenn Sie keine Toleranzen erlauben möchten können Sie diese Spalte auch frei lassen.

3. Flexible Pausenzeiten - Sie können Ihren Mitarbeitern erlauben Ihre Pausen in einer gewissen Zeitspanne zu erlauben. So ist es zum Beispiel erlaubt die Pausen in einem Zeitfenster von 12:30 Uhr bis 14:30 Uhr flexibel zu legen. Das Unternehmen kann auch die Pausenlänge bestimmen. Wenn zum Beispiel eine Pausendauer von einer Stunde definiert wird muss der Mitarbeiter spätestens nach der vorgegebenen Zeit die Pause beenden. Wird die Zeit überschritten wird Ingress dies vermerken. Wenn dies in Ihrem Unternehmen nicht anwendbar ist können Sie diese Eigenschaften ignorieren.

4. Pausenzeiten von der Arbeitszeit ausschließen - Aktivieren Sie das Kontrollkästchen wenn Ihr Unternehmen die Pausenzeiten von der Gesamtarbeitszeit abzieht. Wird dies nicht benötift können Sie das Feld ignorieren.

5. Klicken Sie auf OK um die Einstellungen zu speichern.

Auswahlregeln

Zeitnahme Spanne

Geben Sie eine für die Zeitnahme bestimmte Zeitvorgabe an. Erst dann kan diese als Stechzeit übernommen werden. Haben Sie zum Beispiel Ihre Standard IN-Zeit auf 12:00 Uhr eingestellt werden Aktivitäten vor 12:00 Uhr automatisch als IN-Zeit genommen. Alle Aktivitäten danach als Unterbrechung.

Späteste Zeitnahme

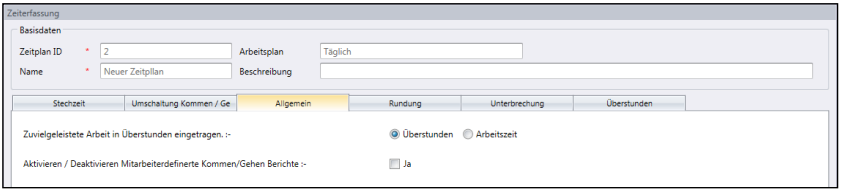
Mit diesem Auswahlfeld können Sie das System so konfigurieren das immer die neueste Aktion in der Zeitnahme als Basis genommen wird. Wenn Ihre Endzeit bei 18:00 Uhr liegt und Sie sich 18:05 Uhr abmelden und 18:10 Uhr erneut anmelden wird die Software immer die aktuellste Zeitnahme in die Auswertung übernehmen. In dem Bespiel wäre das 18:15 Uhr.

BERMERKUNG: *Es wird empfohlen diese Regel nur für Arbeitsbeginn- und ende anwenden. Da diese zwei Spalten nur Ihre letzten Aktionen aufnehmen können.*

Der tägliche Zeitplan kann für rotierende Arbeitspläne verwendet werden. Sie können die Minuten angeben die zur Verschiebung qualifizieren. Das bedeutet das sich der Arbeitsplan im Intervall ändern kann.

Zum Beispiel arbeitet ein Mitarbeiter 4 Tage von 08:00 Uhr bis 16:00 Uhr, fortgesetzt mit 4 Tagen von 16:00 Uhr bis 00:00 Uhr. Der Zyklus wird dann wiederholt.

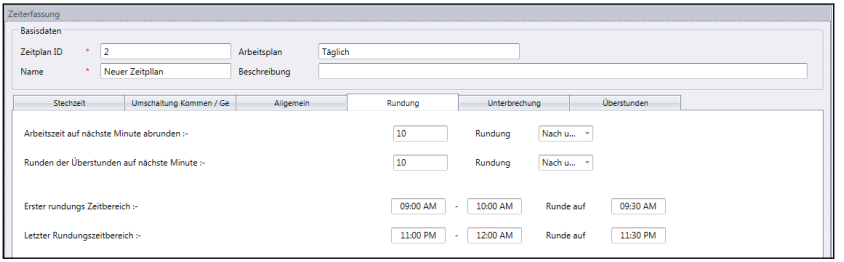
Generelle Regeln



Allgemein sollten Sie bestimmen welche Zeiten in die Überstunden mit einbezogen werden oder als normale Arbeitszeiten gelten. Klicken Sie auf den passenden Button um Ihre Wahl zu bestimmen. Wenn Sie die Zeiten als Überstunden definieren, wird die zusätzliche Zeit des Personals berechnet die diesen Zeitplan verwenden.

Sie können bestimmen das ein Mitarbeiter einen Button betätigen muss um seinen Status während der Zeitnahme zu bestimmen. Klicken Sie auf [JA] wenn Sie das möchten.

Rundungsregeln



Es wird das “runden von Minuten” und das Anzeigen dieser in der Zeittafel bestimmt. Erfahren Sie mehr in nachfolgender Tabelle.

Arbeitszeit runden

Abrunden	Die Arbeitszeit wird im 15 Minuten-Takt aufgerundet: 1-15 Minuten = 15 16-30 Minuten = 30 31-45 Minuten = 45 46-59 Minuten = 1 hour

Abrunden	Die Arbeitszeit wird im 15 Minuten-Takt abgerundet: 1-15 Minuten = 0 16-30 Minuten = 15 31-45 Minuten = 30 46-59 Minuten = 45
Mittelwert	Sobald Sie hier einen Wert einfügen wird die Software den Mittelwert bestimmen. Bei einem Wert von 15 Minuten wird der Mittelwert bei 7 Minuten liegen. Die Zeit für Arbeitsbeginn ist 09:00 Uhr und der Mittelwert leigt bei 07 Minuten. Wenn ein Mitarbeiter in weniger als 07 Minuten nach der eingestelltem Arbeitsbeginn(z. B. 09:07 Uhr) eincheckt, wird die Software die Zeit abrunden (09:00 Uhr). Checkt er erst nach mehr als 7 Minuten ein wird die Software den Wert aufrunden (09:15 Uhr).

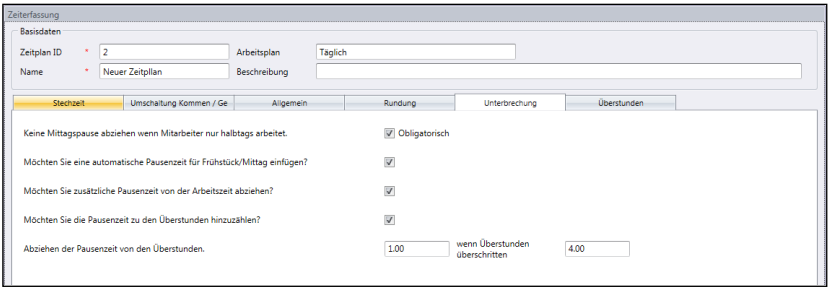
Auf- und Abrunden der Überstunden (Minuten)

Aufrunden	Die Überstunden werden im 15 Minuten-Takt aufgerundet: 1-15 Minuten = 15 16-30 Minuten = 30 31-45 Minuten = 45 46-59 Minuten = 1 hour
Abrunden	Die Überstunden werden im 15 Minuten-Takt abgerundet: 1-15 Minuten = 0 16-30 Minuten = 15 31-45 Minuten = 30 46-59 Minuten = 45
Mittelwert	Sobald Sie hier einen Wert einfügen wird die Software den Mittelwert bestimmen. Bei einem Wert von 30 Minuten wird der Mittelwert bei 15 Minuten liegen. Die Zeit für Überstunden ist 18:00 Uhr und der Mittelwert leigt bei 15 Minuten. Wenn ein Mitarbeiter in weniger als 15 Minuten nach der eingestellten Überstundenzeit (z. B. 18:15 Uhr) auscheckt, wird die Software die Zeit abrunden (18:00 Uhr). Checkt er erst nach mehr als 15 Minuten aus wird die Software den Wert aufrunden (18:30 Uhr).

Erste gerundete Zeitreihe - Diese Funktion wird nur für die Startzeit angewendet. So wird zum Beispiel jede Startzeit von 09:01 Uhr bis 09:15 Uhr auf 09:00 Uhr gerundet.

Letzte gerundete Zeit - Diese Funktion wird nur für die gehen-Zeit angewendet. Sie könne diese Zeit nach Ihren Wünschen von der Software runden lassen. Zum Beispiel wird eine Transaktion zwischen 17:01 Uhr und 17:15 Uhr auf 17:00 Uhrt abgerundet.

Pausenregeln



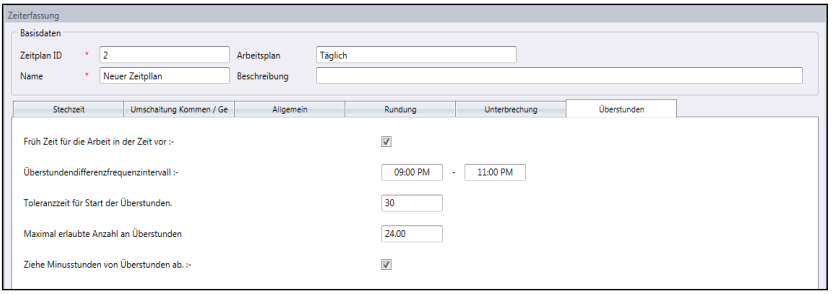
Pause soll die erlaubte Pausenzeit im Zeitplan bestimmen. Ausserdem bestimmen Sie wie die Pausen in der Zeittabellte angezeigt werden.

Erfahren Sie mehr in nachfolgender Tabelle.

Keine Abzug der Mittagszeit bei Halbtagsarbeit	Gibt es spezielle Regeln in Ihrer Firma klicken Sie bitte auf "Prüfen". Verlassen sie die Auswahl wenn dies für Ihre Firma nicht relevant ist.
Wollen Sie eine automatische Pausenzeit hinzufügen wenn Sie diese mit einschließen?	Klicken Sie auf JA wenn Sie die Regel anwenden wollen, das die restliche Pausenzeit der Mitarbeiter die in den Pausen gearbeitet haben in die Arbeitszeit hinzugefügt werden soll.
Wollen Sie die Mittagszeit extra von der Arbeitszeit abziehen?	Klicken Sie auf JA wenn Sie die Pausenzeiten in Stunden beschränken möchten. Extraminuten werden hier von der Gesamtarbeitszeit abgezogen.
Do you want to include lunch/dinner time into overtime hour?	Wenn die Pausen die Endzeit überschreiten können Sie diese in die Überstunden einbeziehen. Verlassen Sie das Fenster wenn dies nicht in Ihrer Firma zur Anwendung kommt.
Pausenzeiten werden von den Überstunden abgezogen.	Wenn Sie die Pausenzeiten von den Überstunden abziehen wollen , definieren Sie hier die Anzahl der Stunden die abgezogen werden sollen enn die genommenden Überstunden einen bestimmten Wert überschreiten.

BEMERKE: *Passen Sie die Regeln nach den Gegebenheiten Ihres Unternehmens an. Lassen Sie es leer wenn keine speziellen Regeln in Ihrem Unternehmen anwenden.*

Überstunden Regeln

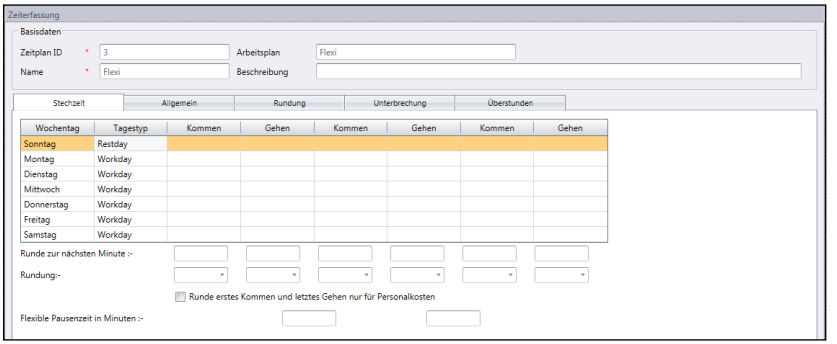


Hier können Sie Überstundenregeln definieren.

Erfahren Sie mehr über die Regeln in nachfolgender Tabelle.

Zu früher Arbeitsbeginn	Manche Mitarbeiter beginnen Ihre Überstunden früher, zum Beispiel statt um 20:00 Uhr kommen sie schon 19:00 Uhr an. Aktivieren Sie das Kontrollkästchen wenn Sie die extra Zeit zu den Überstunden hinzufügen wollen.
Überstundendifferenzial-ratenzwischenraum	Es gibt einige Überstundensitzungen, die von einer Gesellschaft auf wenn Basis erforderlich sind. Definieren Sie Anfangs- und Endzeit für dieser spezifische Überstundensitzungen.
Minimale Anzahl von Minuten die zu Überstunden führen.	Manmal kommt es vor das ein Mitarbeiter nur einige Minuten am Tag mehr arbeitet und dies in die Überstunden einbeziehen möchte. Definieren Sie die Anzahl der Minuten die für Überstunden qualifizieren.
Maximale Anzahl der erlaubten Überstunden.	Setzen Sie eine Grenze welche Anzahl von Überstunden von einem Mitarbeiter gesammelt werden dürfen. Das maximum hier beträgt 24 Stunden.
Minusstunden von Überstunden abziehen.	Es gibt Fälle wo ein Mitarbeiter Überstunden von seiner Gesamtarbeitszeit absetzt. Wenn sie dies erlauben möchten aktivieren Sie das Kontrollkästchen. Die Überstundenregeln in der Liste werden auf jede Gruppe angewendet die in dieser Liste aufgeführt sind. Alle Berechnungen werden in der Zeitübersicht berücksichtigt.

Die flexible Zeitplan



Der flexible Zeitplan ist ein Arbeitsplan der zu spätes einchecken, zu frühes einchecken und Überstunden nicht mit berücksichtigt. Dieser eigent sich bei Gruppen die keinen festen Dienstplan haben.

1. Klicken Sie auf Zeittafel im linken Fenster.
2. Klicken Sie auf Zeittafel Hinzufügen.
3. Geben Sie eine ID ein um die Zeittafel zu verifizieren (1 bis 999).
4. Bennen Sie die Zeittafel.
5. Wählen Sie Flexibel unter Arbeitsplan.
6. Fügen Sie eine Beschreibung der Zeittafel ein.
7. Klicken Sie auf OK

Zeitplanungsregeln

Die Zeitnahme erfordert eine Aktivität des Mitarbeiters am jeweiligen Zeitnahmegerät. Ingress bietet 6 Anwesenheitsspalten in 3 Paaren an.

1. Definieren Sie den Tagestyp für jede Reihe.
2. Runden zur nächsten Minute: In jeder Zeitspalte könne Sie zur nächtsten Minute Runden lassen sollte dies in Ihrem Unternehmen so gehandhabt werden. Nachfolgend finden Sie Beispiele wie dies anzuwenden ist.

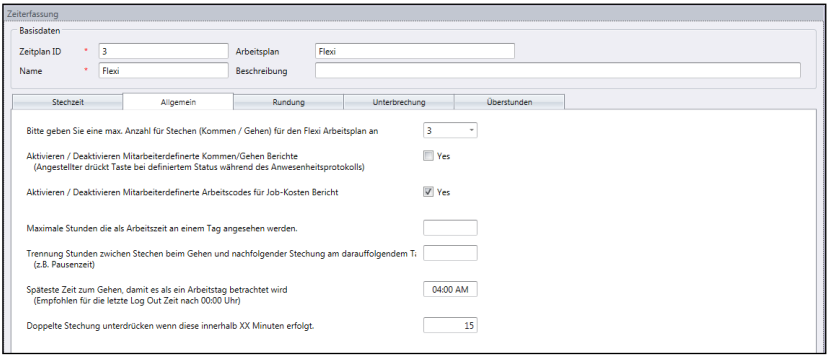
   Aufrunden: Wenn Sie “aufrunden 15 Minuten” auswählen wird die Zeit um 15 Minuten aufgerundet. Zum Beispiel ein Zeit von 09:06 Uhr wird auf 09:15 Uhr gerundet.

   Abrunden: Wenn Sie “abrunden 15 Minuten” auswählen wird die Zeit um 15 Minuten abgerundet. Zum Beispiel ein Zeit von 09:06 Uhr wird auf 09:00 Uhr gerundet.

   Mittelwert: Wenn Sie “Mittelwert” auswählen wird die Durchschnittszeit genommen. Zum Beispiel ein Zeit von 09:06 Uhr wird auf 09:07 Uhr festgelegt.

3. Flexible Pausenzeiten
4. Diese Einstellung erlaubt es Unternehmen bestimmte Pausenzeiträume festzulegen. So werden zum Beispiel Pausen im zeitraum von 12:30 Uhr bis 14:30 Uhr berücksichtigt. Während dieses Zeitraumes können Mitarbeiter Ihre Pausenzeit frei bestimmen. Wenn das Unternehmen eine Pausenspanne von 1 Stunde setzt muss der Mitarbeiter der 13:00 Uhr Pause macht seine Arbeit um 14:00 fortsetzen. Wenn der Mitarbeiter diese Zeit überschreitet wird Ingress eine Bemerkung hinzufügen. Verlassen Sie diese Einstellung wenn dies auf Ihr Unternehmen nicht anwendbar ist.
5. Es gibt einen Button wo Sie auswählen können wie der Arbeitsbeginn und das Arbeitsende gerundet werden sollen. Verlassen Sie dieses Feld wenn Sie die Funktion nicht benötigen.
6. Klicken Sie auf OK, um die Einstellungen zu speichern.

Generelle Regeln


Zeiterfassung
Basisdaten
Zeitplan ID * 3
Arbeitsplan Flexi
Name * Flexi
Beschreibung
Stechzeit
Allgemein
Rundung
Unterbrechung
Überstunden
Bitte geben Sie eine max. Anzahl für Stechen (Kommen / Gehen) für den Flexi Arbeitsplan an
3
Aktivieren / Deaktivieren Mitarbeiterdefinerte Kommen/Gehen Berichte
(Angestellter drückt Taste bei definiertem Status während des Anwesenheitsprotokolls)
Yes
Aktivieren / Deaktivieren Mitarbeiterdefinerte Arbeitscodes für Job-Kosten Bericht
Yes
Maximale Stunden die als Arbeitszeit an einem Tag angesehen werden.
Trennung Stunden zwichen Stechen beim Gehen und nachfolgender Stechung am darauffolgendem T
(z.B. Pausenzeit)
Späteste Zeit zum Gehen, damit es als ein Arbeitstag betrachtet wird
(Empfohlen für die letzte Log Out Zeit nach 00:00 Uhr)
04:00 AM
Doppelte Stechung unterdrücken wenn diese innerhalb XX Minuten erfolgt.
15

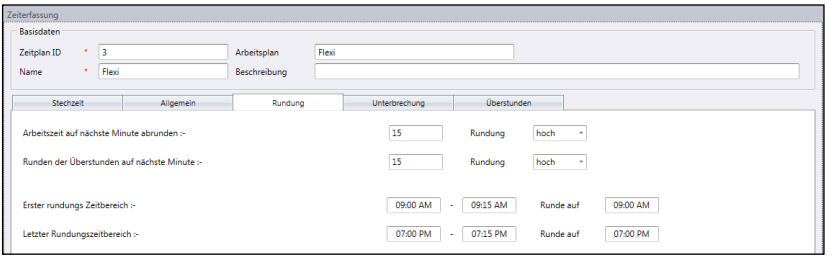
Es gibt allgemeine Regeln zum setzen von Flxiarbeitszeiten. Weil der Mitarbeiter der diese nutzt nicht den normalen Arbeitsplänen zugeordnet wird.

Erfahren Sie mehr über die Regelungen des flexiblen Zeitplans in nachfolgender Tabelle:

Regeln	Beschreibungen
Bitte legen Sie die maximale Anzahl von kommen und gehen Paaren in dem Flexiplan fest.	Die maximale Anzahl von Zeitaktionen in TCMS V2 ist auf 3 begrenzt (Arbeitsbeginn/Arbeitsende, Pausenbeginn/Pausenende, Überstunden/geleistete Überstunden) In der Flexiarbeitszeit können Sie nur eine oder einige Paarung en davon bestimmen.
Aktivieren/Deaktivieren eines Benutzers	Klicken Sie auf JA wenn Sie wollen das der Benutzer den relevanten Knopf drückt um seinen Status genau zu definieren. Wenn Sie diese Eigenschaft deaktiviert lassen wird das System die Daten automatisch in die passenden Spalten übertragen. Klicken Sie auf JA wenn Sie wollen dass der Mitarbeiter einen Arbeitscode eingeben muss um sein Aufgabe konkret zudefinieren.

Regeln	Beschreibungen
Aktivieren und Deaktivieren von Nutzerarbeitscodes für Arbeitskostenaufzeichnung.	Klicken Sie auf JA wenn Sie wollen das ein Mitarbeiter einen Arbeitscode eingibt um seine Tätigkeit zu spezifizieren.
Maximale Arbeitsstunden an einem Arbeitstag	Es gibt Fälle an denen Mitarbeiter spät abends arbeiten undsich die Arbeitszeit bis in den nächsten Tag erweitert. Um in diesen Fällen Verwirrung zu vermeiden müssen Sie die maximale Arbeitszeit an einem Werktag, der in den anderen übergeht, angeben. Zum Beispiel wenn der Mitarbeiter 22:00 Uhr beginnt und die maximale Arbeitszeit 08:00 Stunden beträgt muss er spätestens 06:00 Uhr am Folgetag enden.
Stundenauszug zwischen Arbeitsbeginn und Arbeitsende um sich für den nächsten Arbeitstag zu qualifizieren.	Im Anschluss an die Regeln oben müssen Sie die Dauer zwischen Kommen und Gehen bestimmen um einen Mitarbeiter für eine folgende Tagesbezahlung zu qualifizieren. Zum Beispiel wenn der Mitarbeiter 18:00 Uhr auscheckt muss er sich nicht sofort wieder einchecken um den nächsten Tag als Arbeitszeit zu betrachten.
Späteste gehen-Zeit an einem Arbeitstag	Wenn ein Mitarbeiter spät abends mit der Arbeitszeit beginnt und die Arbeitsstunden strecken sich bis in den nächsten Tag, wird dies als derselbe Werktag betrachtet. Sie müssen hierzu die Zeiten angeben die für den gleichen Werktag berechtigen.
Doppelte Aktivitäten der fortlaufenden Zeitnahme wenn diese innerhalb von Minuten ist.	Alle Zeitnahme Aktionen innerhalb dieses Zeitintervalls werden nur einmal geprüft. Zum Beispiel bei einem Arbeitszeitbeginn von 09:00 Uhr mit einem Zeitabstand von 15 Minuten wird jede Aktion innerhalb der 15 Minuten als rechtzeitiger Arbeitsbeginn gewertet.

Rundungsregeln



Es wird das “runden von Minuten” und das Anzeigen dieser in der Zeittafel bestimmt.

Sie mehr in nachfolgender Tabelle.

Arbeitszeiten runden

Aufrunden	Die Arbeitszeit wird im 15 Minuten-Takt aufgerundet: 1-15 Minuten = 15 16-30 Minuten = 30 31-45 Minuten = 45 46-59 Minuten = 1 hour
Abrunden	Die Arbeitszeit wird im 15 Minuten-Takt abgerundet: 1-15 Minuten = 0 16-30 Minuten = 15 31-45 Minuten = 30 46-59 Minuten = 45
Mittelwert	Sobald Sie hier einen Wert einfügen, wird die Software den Mittelwert berechnen. Zum Beispiel, wenn Sie den Wert auf 15 Minuten eingestellt haben, würde der Mittelwert 7 Minuten sein. Beim kommen liegt der Zeitplan bei 09:00 Uhr und der Mittelwert beträgt 7 Minuten. Wenn der Benutzer in weniger als 7 Minuten nach der Kommen-Zeit eincheckt,zum Beispiel 09:07 Uhr, wird die Software die Transaktionsdaten auf 09:00 Uhr abrunden. Wenn der Benutzer nach den 7 Minuten eincheckt, wird die Software dieTransaktionsdaten auf 09:15 Uhr aufrunden.

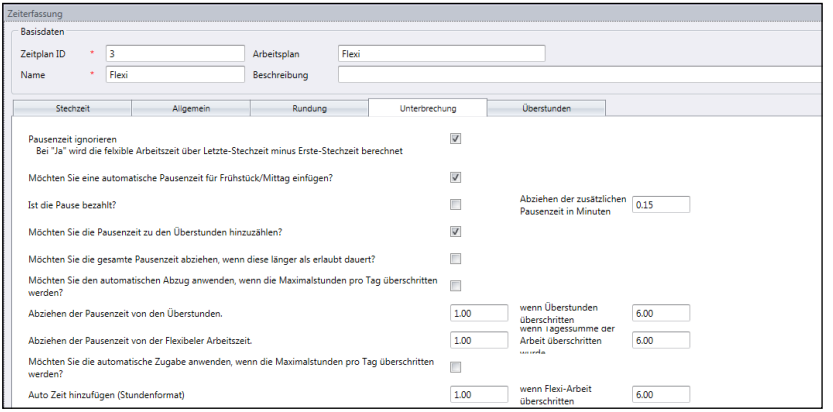
Auf- und Abrunden der Überstunden

Aufrunden	Die Überstunden werden im 15 Minuten-Takt aufgerundet: 1-15 Minuten = 15 16-30 Minuten = 30 31-45 Minuten = 45 46-59 Minuten = 1 hour
Abrunden	Die Überstunden werden im 15 Minuten-Takt aufgerundet: 1-15 Minuten = 0 16-30 Minuten = 15 31-45 Minuten = 30 46-59 Minuten = 45
Mittelwert	Sobald Sie hier einen Wert einfügen, wird die Software den Mittelwert berechnen. Zum Beispiel, wenn Sie den Wert auf 30 Minuten eingestellt haben, würde der Mittelwert 15 Minuten sein. Bei Überstunden liegt der Zeitplan bei 18:00 Uhr und der Mittelwert beträgt 15 Minuten. Wenn der Benutzer in weniger als 15 Minuten nach der Überstundenzeit auscheckt, zum Beispiel 18:15 Uhr, wird die Software die Transaktionsdaten auf 18:00 Uhr abrunden. Wenn der Benutzer nach den 15 Minuten auscheckt, wird die Software die Transaktionsdaten auf 18:30 Uhr aufrunden.

Erste gerundete Zeitreihe - Diese Funktion wird nur für die Startzeit angewendet. So wird zum Beispiel jede Startzeit von 09:01 Uhr bis 09:15 Uhr auf 09:00 Uhr gerundet.

Letzte gerundete Zeitreihe - Diese Funktion wird nur für die Endzeit angewendet. So wird zum Beispiel jede Endzeit von 17:01 Uhr bis 17:15 Uhr auf 17:00 Uhr gerundet.

Pausenregeln



Pause soll die erlaubte Pausenzeit im Zeitplan bestimmen. Ausserdem bestimmen Sie wie die Pausen in der Zeittabellte angezeigt werden.

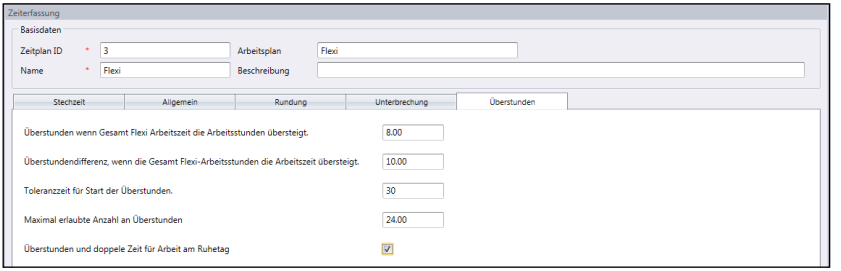
Sie mehr in nachfolgender Tabelle.

Pausenzeiten ignorieren	Klicken Sie auf JA wenn Sie die Pausenzeiten von der Gesamtarbeitszeit abziehen wollen. Wenn Sie dieses Feld nicht aktivieren wird wird aus Einstechzeit und Ausstechzeit die Arbeitszeit berechnet.
Wollen Sie eine automatische Pausenzeit hinzufügen wenn Sie diese mit einschließen?	Klicken Sie auf JA wenn Sie die Regel anwenden wollen, das die restliche Pausenzeit der Mitarbeiter die in den Pausen gearbeitet haben in die Arbeitszeit hinzugefügt werden soll.
Wird die Pause bezahlt? Ziehen Sie die Gesamte Pause in Minuten ab.	Klicken Sie auf JA wenn Sie die Pausenzeiten in die Gesamtarbeitszeit einschließen wollen. Wenn nicht wird die Pausenzeit von der Gesamtarbeitszeit abgezogen. Sie müssen jedoch die Gesamtpausenzeit angeben die ein Mitarbeiter nehmen kann. Wenn diese Pausenzeiten überschritten werden, werden zusätzliche Minuten von der Gesamtarbeitszeit abgezogen.

Wollen Sie Pausenzeiten in die Überstunden einbeziehen?	Klicken Sie auf JA wenn Sie die Pausenzeiten in die Überstunden einbeziehen wollen.
Wollen Sie die Pausenzeiten ausschließen wenn diese größer sind als erlaubt?	Wenn Sie bei dieser Funktion auf JA klicken werden dem Mitarbeiter bei überzogener Pausenzeit die Gesamtpausenzeiten von den Gesamtarbeitsstunden abgezogen. Zum Beispiel wenn ein Mitabeiter eine Gesamtarbeitszeit von 8 Stunden hat und eine Pause von 01:30 Stunden nimmt wird die Software bei einer erlaubten Pausenzeit von einer Stunde diese eine Stunden von der Gesamtarbeitszeit abziehen.
Wollen Sie einen automatischen Abzug von den Gesamtarbeitsstunden erlauben?	Geben Sie die Stunden der Pausenzeiten von den Überstunden an wenn die vorgegebenen Werte der Überstunden in den Spalten überschritten wurden. Wenn Sie 1 Stunde und 8 Stunden einstellen bedeutet dies, dass der Mitarbeiter Überstunden in Höhe von 9 Stunden nimmt eine Stunden Pausenzeit abgezogen werden und sich die Gesamtüberstunden auf 8 Stunden verringern.
Ziehen Sie die Pausenzeiten von den Flexizeiten ab wenn die Flexizeiten überschritten wurden.	Geben Sie die Stunden der Pausenzeiten von den Flexistunden an wenn die vorgegebenen Werte der Flexistunden in den Spalten überschritten wurden. Wenn Sie 1 Stunde und 8 Stunden einstellen bedeutet dies, dass der Mitarbeiter Flexistunden in Höhe von 9 Stunden nimmt eine Stunde Pausenzeit abgezogen werden und sich die Gesamtflexistunden auf 8 Stunden verringern.
Automatische Zeit einfügen (im Stundenformat) wenn es die Flexizeit übersteigt.	Geben Sie die Zeit für die Pausen in der flexiblen Arbeitszeit an. Wenn Sie eine Stunde angeben wird die Soft automatisch eine Stunde zur Gesamtflexizeit hinzufügen.

BEMERKE: *Geben Sie die Regeln gemäß Ihrer Unternehmenspolitik an. Lassen Sie dieses Feld offen wenn dies in Ihrem Unternehmen nicht anwendbar ist.*

Überstundenregeln



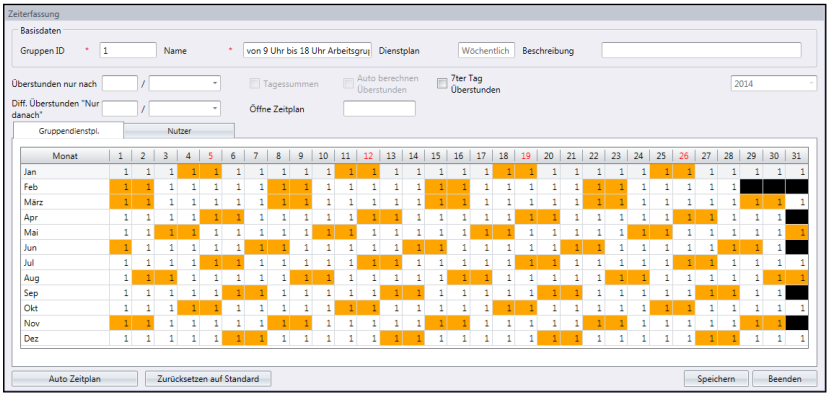
Pause soll die erlaubte Pausenzeit im Zeitplan bestimmen. Ausserdem bestimmen Sie wie die Pausen in der Zeittabellte angezeigt werden.

Erfahren Sie mehr in der folgenden Tabelle:

Überstunden wenn die komplette Flexizeit für gewisse Stunden überschritten wird.	Definieren Sie die Standardarbeitszeit für die flexiblen Arbeitszeiten. zum Beispiel 8 Stunden. Wenn ein Mitarbeiter diese überschreitet wenn darauffolgende Stunden als Überstunden betrachtet.
Unterschiedliche Überstundenmodelle wenn die flexible Arbeitszeit überschritten wird.	In manchen Unternehmen ist geregelt das ein Mitarbeiter einen gewisse Überstundenrate einhalten müssen. Definieren Sie hier die Rate die den Mitarbeiter für Überstunden qualifiziert.
Minimale Anzahl der Zeit zur erzeugung von Überstunden.	Es kommt vor das ein Mitarbeiten nur ein paar Minuten über die Regelarbeitszeit kommt. Definieren Sie ab welcher Überschreitung der Regelarbeitszeit Überstunden erzeugt werden.
Maximal erlaubte Überstunden	Setzen Sie eine Grenze für Überstunden die von einem Mitarbeiten gesammelt werden dürfen. Das maximum hierbei beträgt 24 Stunden.
Überstunden & doppelte Arbeitszeit an Ruhetagen	In einigen Unternehmen werden den Mitarbeitern Überstunden bezahlt oder die doppelte Zeit berechnet wenn sie ausserhalb von Werktagen arbeiten. Wenn Sie dies erlauben möchten aktivieren Sie das Kontrollkästchen.

Zu Beachten: *Der Überstundenregelsatz wird auf jede Gruppe der Liste angewandt. Alle Reglen werden in der Zeittafel für das Personal angewandt.*

Aufbau von Dienstplan-Gruppe

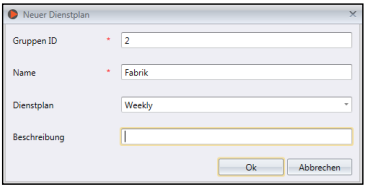


Fügen Sie die Zeittafeln in den Gruppendienstplan hinein, um einen kompletten Arbeitskalender zu generieren. Benutzer werden zu dem gleichen Gruppendienstplan zugeordnet, wenn sie den gleichen Zeittafeln folgen.

Es gibt 2 Typen von Gruppendienstplänen:

- WÖCHENTLICH - Wochengruppendienstplan. Dieser ist Weltweit am meisten verwendet, wo Arbeitstage den Wochentagen und Freie Tageauf das Wochendende entfallen.
- VERSCHIEBEN - täglicher Standardarbeitsplan. Dieser ist geeignet für vielfache Verschiebungen (offen, Nacht, Rotation). Perfekt für Unternehmen wo sich Arbeitspläne täglich ändern.

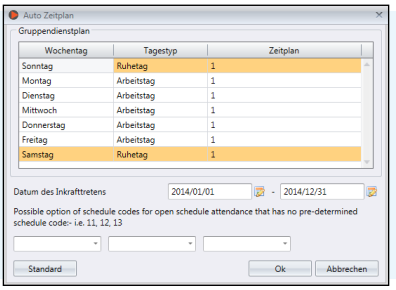
Erstellen eines wöchentlichen Gruppendienstplanes



1. Klicken Sie auf Gruppendienstplan im linken Feld.
2. Klicken Sie auf Dienstplan hinzufügen.
3. Wählen Sie eine Nummer für das Gruppenarbeitsschema aus.

4. Name des Gruppen-Dienstplans, z.B. 9.00 Uhr bis 18.00 Uhr.
5. Klicken Sie auf Bearbeiten unter der Registerkarte Gruppe-Dienstplan.
6. Wählen Sie den wöchentlichen Dienstplan aus.
7. Klicken Sie OK um fortzufahren
8. Klicken Sie auf Bearbeiten.
9. Klicken Sie auf Stundenplan hinzufügen.

   Jetzt können Sie den Zeitplan für den Dienstplan auswählen.



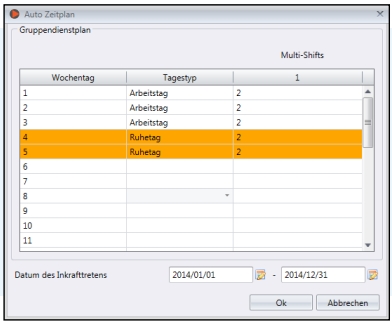
1. Definieren Sie die Art des Tages.
2. Wählen Sie Zeittafel aus.
3. Definieren Sie das Datum des Inkrafttretens, um den Kalender anzulegen.
4. Klicken Sie auf OK, um die Einstellungen zu speichern.

“Jetzt können Sie den Gruppendienstplan verwenden. Im nächsten Schritt können Sie die Mitarbeiter hinzufügen die diesem Dienstplan angehören.”

Erstellen eines Gruppendienstplanes

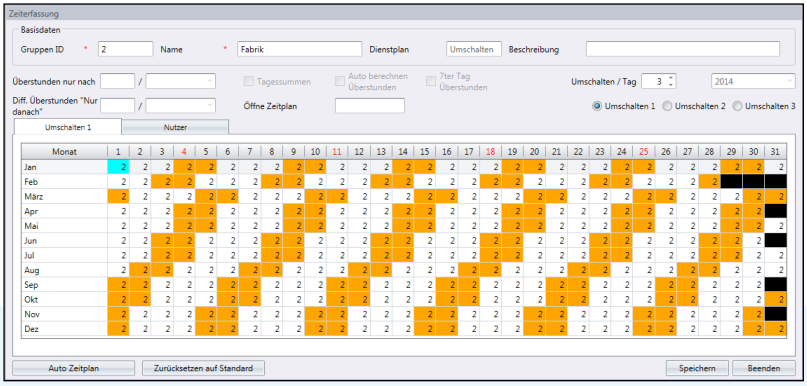
1. Klicken Sie auf Gruppendienstplan im linken Feld.
2. Klicken Sie auf Dienstplan hinzufügen.
3. Wählen Sie eine Nummer für den Gruppendienstplan.
4. Benennen Sie den Gruppendienstplan.
5. Klicken Sie auf Bearbeiten unter der Registerkarte Gruppe-Dienstplan.
6. Wählen Sie Dienstplan ändern.
7. Klicken Sie auf OK um fortzufahren.
8. Klicken Sie auf Bearbeiten.
9. Klicken Sie auf Stundenplan hinzufügen.

   Jetzt können Sie den Zeitplan für den Dienstplan auswählen.



1. Definieren Sie Sie den Tagestyp gemäß den Verschiebungsregeln, zum Beispiel 3 Arbeitstage gefolgt von einem Resttag.
2. Wählen Sie die Zeittafel aus, um zu folgen (tägliche Liste verwenden)
3. Definieren Sie den Tag des Inkrafttretens um den Kalender anzuwenden.
4. Klicken Sie auf OK, um die Einstellungen zu speichern.

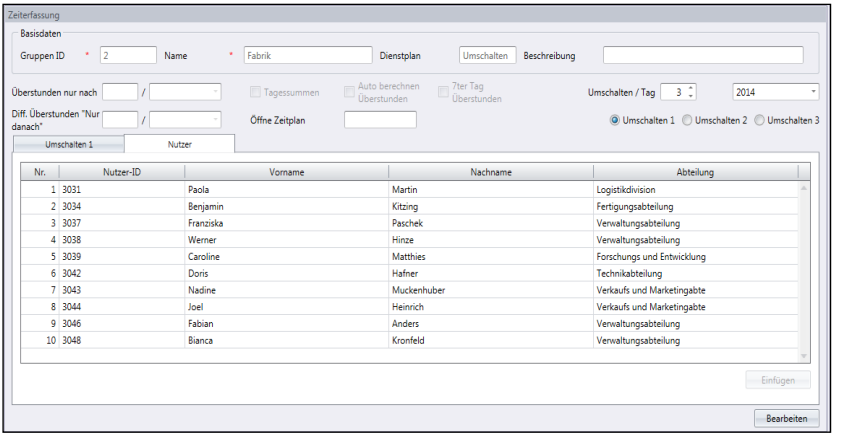
Die Software unterstützt bsi zu 3 Verschiebungen pro Tag:



1. Klicken Sie auf ***Bearbeiten***.
2. Ändern Sie den Wert von 1 bis 2 oder unter der Abteilung der ***Verschiebung/Tag***
3. Klicken Sie auf ***Auto-Zeitplan*** um zusätzliche Spalten anzuzeigen in denen Sie den Termincode für jeden Werktag eingeben können.

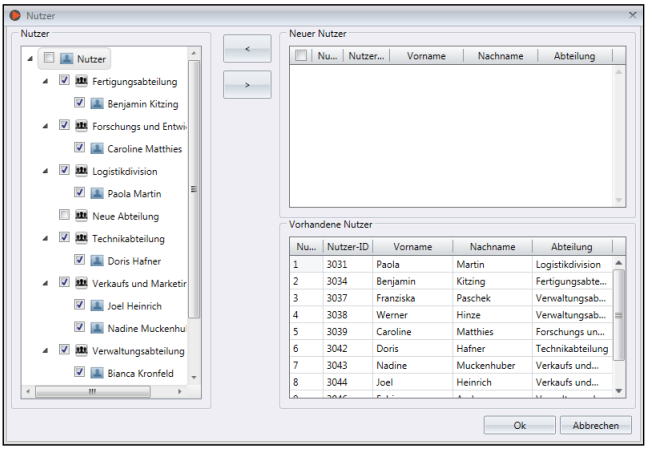
Jetzt haben Sie das Gruppenarbeitsschema komplett und es ist zur Verwendung bereit. Im nächsten Schritt könne Sie die Beutzer hinzufügen die nach den selben Regeln arbeiten.

Weisen Sie die Benutzer em Gruppen-Dienstplan zu



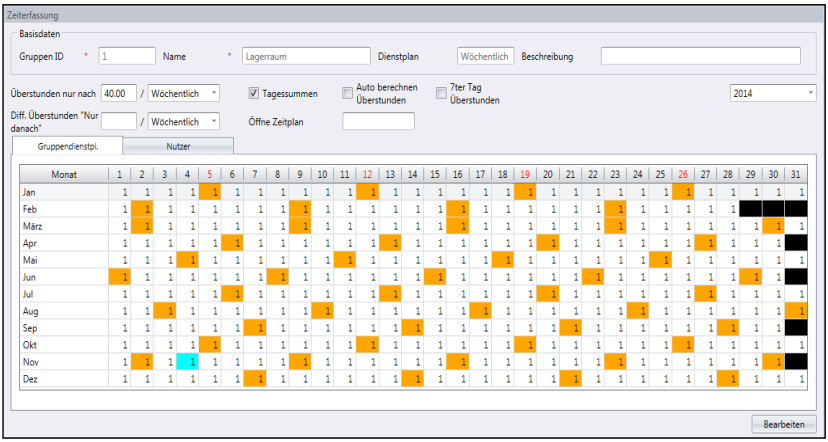
Sie können nun die Benutzer zu Gruppen-Dienstplänen zuordnen. Sie können einzelne Benutzer oder alle Benutzer aus einer Abteilung auswählen.

1. Klicken Sie auf Bearbeiten unter der Benutzer Registerkarte.
2. Klicken Sie auf Hinzufügen um einen Mitarbeiter zum Gruppendienstplan hinzuzufügen.



3. Wählen Sie die Benutzer, um sie zum Gruppen-Dienstplan hinzufügen. Sie können Benutzer individuell oder abteilungsweise auswählen.
4. Klicken Sie auf OK, um die Einstellungen zu speichern.

Spezielle Arbeitsregeln



Sie können bis zu 5 verschiedene Arbeitsregeln definieren.

- Überstunden nur danach - Ingress sammelt die Arbeitszeit der Mitarbeiter in einem bestimmten Zeitabschnitt an, bevor er Überstunden während eines bestimmten Zeitabschnitts (wöchentlich, monatlich, usw) sammeln kann.

  Beispiel: Wenn die bestimmte Arbeitszeit für die Woche auf 40 Stunden festgelegt ist und ein Mitarbeiter 45 Stunden arbeitet, veranlasst die Software das 40 Stunden als Arbeitszeit und 5 Stunden als Überstunden gewertet werden.

  Sie können eine zusätzliche Auswahl anwenden um Überstunden entsprechend anzusehen.

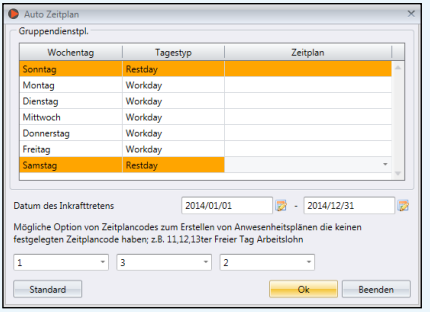
  Tägliche Summen: Ingress zeigt zusätzliche Spalten im Zeitplan an wenn diese Option aktiviert ist. Diese Spalte zeigt individuell für jeden Mitarbeiter die geleistete Arbeitszeit und Überstunden an. Die schlussendliche Berechnung erfolgt jedoch danach.

  Automatisch berechnete Überstunden: Diese Auswahl gleicht der täglichen Summe der Überstunden. Sie dient ausschließlich zum Anzeigen der täglichen Überstunden.

  7 Tage Überstunden: Diese Auswahl wird nur aktiv wenn Sie diese Überstundenregel anwenden. Die Software berechnet nur Überstunden wenn Mitarbeiter 7 Tage am Stück kontinuierlich arbeiten. Im Falle das der Mitarbeiter 7 Tage keine Arbeit ausführt wir die Software.

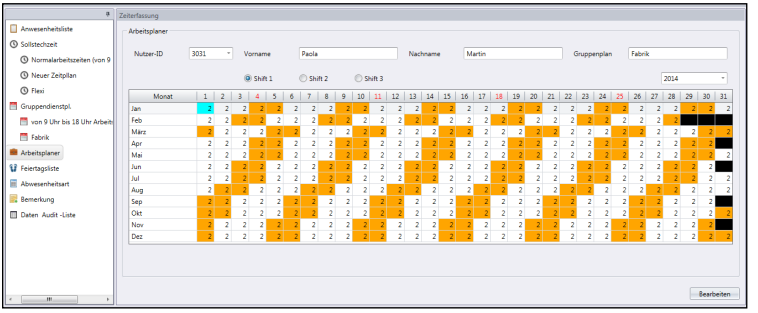
- Offener Zeitplan - Dieser Offene Zeitplan ist für Unternehmen bestimmt die keinen speziellen Zeit- oder Dienstplan festlegen wollen. In diesem Fall wird die Software die Zeitnahmen des Mitarbeiters innerhalb des definierten Rahmens einordnen. Dieser Rahmen muss klar definiert sein da nachträglich nichts manuell verändert werden kann. Die Software ist nicht in der Lage dem Benutzer einer Verschiebung zuzuteilen wenn die Zeiten sich überlappen.

Bestimmen Sie eine Code für den Zeitplan wenn Sie das Gruppenarbeitsschema konfigurieren.



1. Definieren Sie eine ***Auto-Zeittafel***.
2. Definieren Sie den ***Tagestyp***.
3. Verlassen Sie das ***Zeitplanfenster***.
4. Definieren Sie den ***Datrumsbreich*** für den Dienstplan.
5. Wählen Sie einen Code für den Zeitplan (max. 3)
6. Klicken Sie auf ***OK*** um die Einstellungen zu speichern.

Benutzer Dienstplan

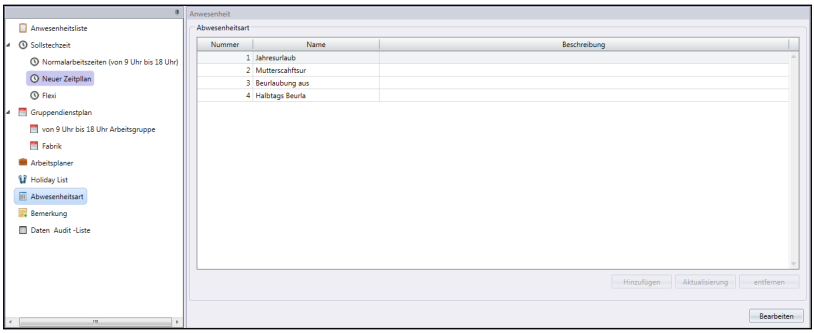


Sie können den Arbeitskalender eines Benutzers ändern, ohne für ihn einem neuen Gruppendienstplan zu erstellen. Sie können die gültigen Zeittafeln für diesen Benutzer unter dem gleichen Gruppendienstplan ändern.

1. Klicken Sie auf Benutzer-Dienstpaln im linken Feld.
2. Doppelklicken Sie auf die Benutzer-ID, um den Gruppendienstplan anzupassen.
3. siehe Kapitel 7.2.1 • Erstellen von Gruppendienstplan, um einen individuellen Arbeitskalender zu erstellen.

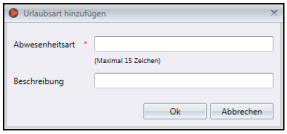
Abwesenheit und Bemerkungen

Hinzufügen von Abwesenheitsarten



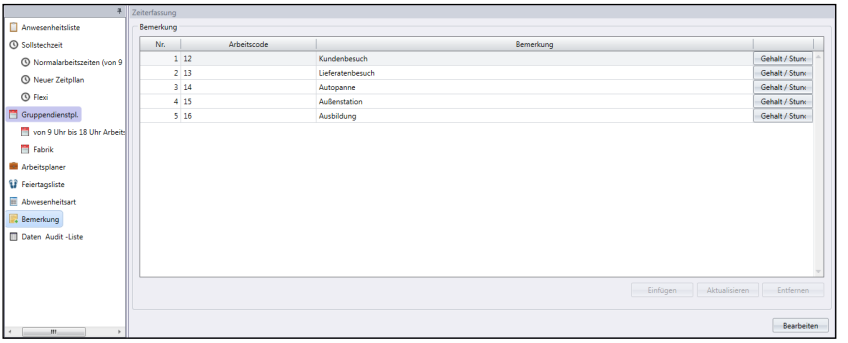
Sie können eine Liste von Abwesenheitsarten in Ingress erstellen. Sie können Abwesenheitszeiten in der Anwesenheitsliste anzeigen.

1. Wählen Sie Abwesenheitstyp aus der linken Seite.
2. Klicken Sie auf Bearbeiten.
3. Klicken Sie auf Hinzufügen.



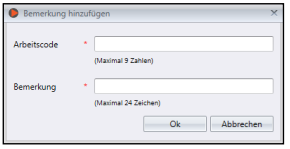
4. Benennen Sie den Abwesenheitstyp.
5. Fügen Sie eine Beschreibung für diese Abwesenheitsart hinzu.
6. Klicken Sie auf OK, um den neuen Abwesenheitstyp in Liste einzufügen.
7. Klicken Sie auf Speichern, um die Einstellungen zu speichern.

Hinzufügen von Bemerkungen



Während der Verifizierung können die Benutzer an verschiedenen Terminals einen Grund für außergewöhnliche Anwesenheitsgründe eingeben. Zum Beispiel gibt Benutzer 10 ein, um zu zeigen, dass er zur Arbeitsstelle spät gekommen ist, weil er außerhalb eine Geschäftskonferenz besucht hat. Sie können die Liste der Kurzbezeichnungen unter der Spalte [Anmerkung] erstellen und oder auch eine Bemerkung in die Anwesenheitsliste eingeben, um seine Anwesenheitslisten zu beschreiben.

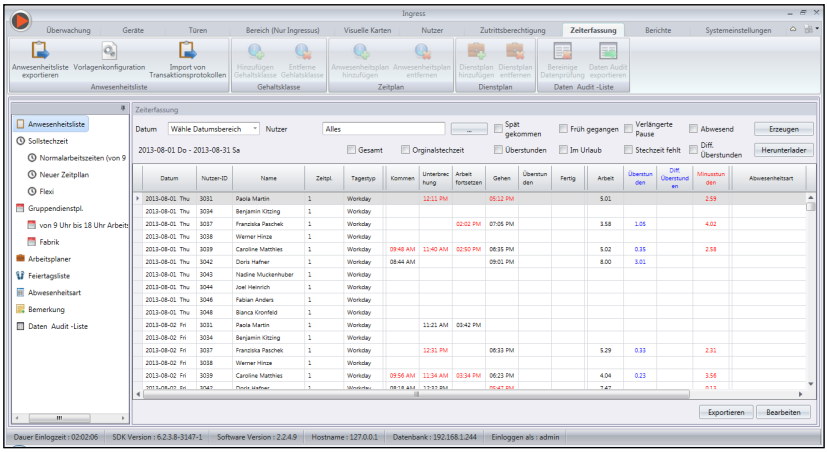
1. Klicken Sie auf Anmerkung auf der linken Seite.
2. Klicken Sie auf Bearbeiten.
3. Klicken Sie auf Hinzufügen.



4. Setzen Sie eine Nummer unter Kurzbezeichnung ein, die beim Gerät während der Verifizierung verwendet werden soll), z.B. 15.
5. Geben Sie der Kurzbezeichnung eine kurze Beschreibung unter Anmerkung, z.B. Außenstelle.
6. Klicken Sie auf OK, um die neue Kurzbezeichnung in der Liste zu speichern.
7. Klicken Sie auf Speichern, um die Einstellungen zu speichern.

Anwesenheitsliste

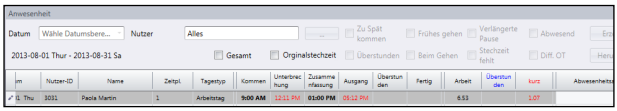
Anzeigen und Bearbeiten



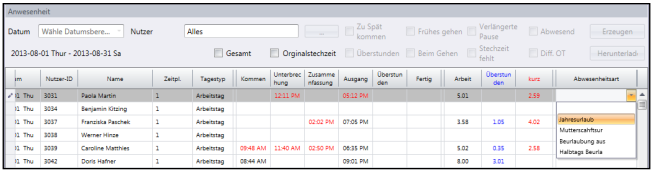
Anwesenheitsliste zeigt die Aufzeichnungen aller Benutzers. Sie sehen die IN-OUT Aufzeichnungen, Arbeitszeit , Kurzzeit, Überstunden und Abwesenheit. Sie können diese detailliert unter folgenden Rubriken ansehen:

- Datumsbereich
- Abteilung
- Spät rein
- Früh raus
- Erweiterte Pause
- Abwesend
- Überstunden
- auf Urlaub
- Fehlzeiten

Ingress bietet Flexibilität für die Administratoren, die Anwesenheitslisten zu ändern. Aufzeichnungen fett dargestellt zeigen an, dass Änderungen durchgeführt wurden. Sie können den Urlaub, der vom Benutzern genommen wurde, einfügen(unter Urlaubsyp Spalte) oder setzen Sie einen Hinweis zu seinen Aufzeichnungen (unter Anmerkung Spalte).



1. Klicken Sie auf Bearbeiten.
2. Geben Sie die Zeit in die entsprechenden Spalten ein.
3. Arbeitszeit , Kurzzeit und Überstunden werden automatisch anhand der Zeittafel berechnet.
4. Klicken Sie auf Speichern um die Einstellungen zu speichern.

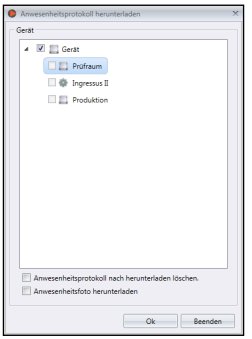


1. Klicken Sie auf Bearbeiten.
2. Gehen Sie zur Spalte Abwesenheitstyp oder Anmerkung.
3. Wählen Sie Abwesenheitsart oder Bemerkung.
4. Klicken Sie auf Speichern, um die Einstellungen zu speichern.

Herunterladen von Daten von Geräten

Bevor Sie Anwesenheitsdaten anschauen, ist es ratsam, die Daten aller Geräte herunterzuladen. Anwesenheitsliste aktualisiert die Datensätze, wenn neue Daten in die Datenbank geladen werden.

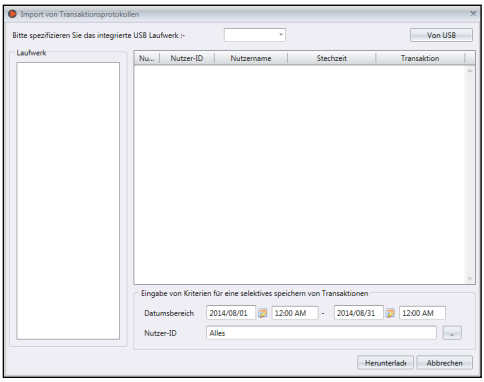
1. Klicken Sie Herunterladen in der Anwesenheitsliste.



2. Wählen Sie die Geräte aus, um daraus die Daten herunterzuladen.
3. Es ist empfohlen Entfernen Sie Transaktionsprotokolle nach dem Herunterladen zu klicken. Ingress löscht alle Protokolle in Geräten nach Abschluss des Herunterladens von den Geräten. Dieser Vorgang vermeidet einen Datenüberfluss im Protokollspeicher des Gerätes.
4. Klicken Sie auf OK, um fortzufahren.

Wenn die TCP / IP oder RS485-Verbindung nicht verfügbar ist, können Sie die Transaktionsprotokolle mit Hilfe eines USB-Sticks von Geräten herunterladen. Führen Sie hierfür die folgenden Schritte durch:

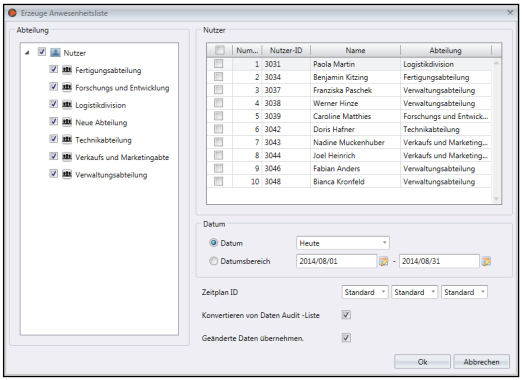
1. Klicken Sie auf Import-Transaktionsprotokollen.



2. Geben Sie die Position des Laufwerkes des USB-Flash-Disk an.
3. Klicken Sie auf Von USB.
4. Definieren Sie den Datum-Bereich von Daten, die zu Ingress importiert werden sollen.
5. Wählen Sie die Benutzer-ID.
6. Klicken Sie auf Herunterladen, um fortzufahren.

Erstellen von Anwesenheitsdaten

Starten Sie generiere Anwesenheitsdaten, damit Ingress die Anwesenheistsliste neu erstellt und neu berechnet. Sie müssen Anwesenheitsdaten generieren, nachdem Sie die Änderungen in der Zeittafel oder im Gruppendienstplan gemacht haben. Die Änderungen werden erst nach diesem Prozess wirksam.



1. Klicken Sie auf Erstellen auf Anwesenheitsliste.
2. Wählen Sie Benutzer-ID.
3. Wählen Sie Datumsbereich.
4. Wählen Sie nur die Zeitplan-ID aus, für die Ingress die Anwesenheitslisten nach einer neuen Zeittafel generieren soll.

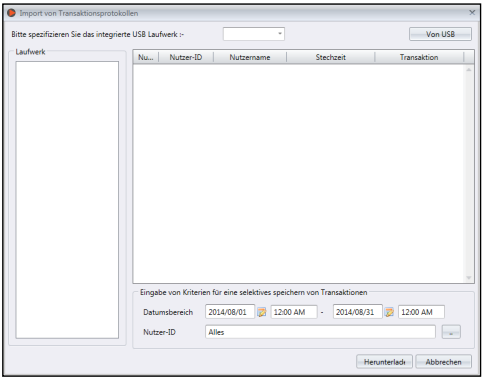
5. Bestätigen Sie Konvertieren von Datenprüf-Liste, so wird Ingress die Datenbank auf neue Aufzeichnungen überprüfen.
6. Klicken Sie auf geänderte Daten des Benutzers behalten, so wird Ingress keine bearbeiteten Aufzeichnungen löschen, die davor gemacht worden sind.
7. Klicken Sie auf OK, um fortzufahren.

Export Anwesenheitsliste

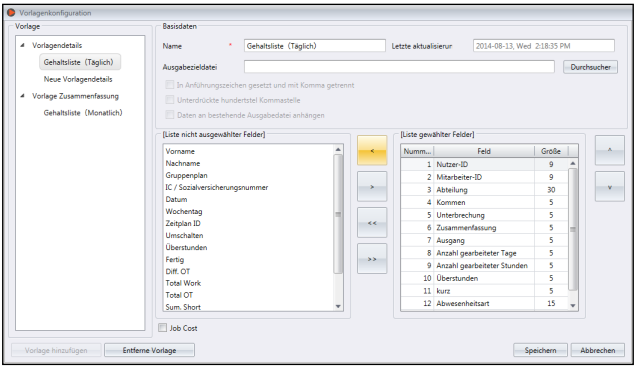
Sie können die Anwesenheitslisten für die weitere Verwendung zu Lohnabrechnungs-Software exportieren. Die exportierten Datensätze können detaillierte (Tag-für-Tag) oder zusammengefasst sein. Sie können die Ausgabedatei, die von der Lohnabrechnungs-Software verwendet werden soll im XLS-oder TXT-Format speichern.

Bevor Sie Anwesenheitslisten exportieren, müssen Sie eine Vorlage für das Export-Format konfigurieren und zu exportierenden Datenfelder und ihre Länge bestimmen. Sie können mehrere Vorlagen konfigurieren, wenn Sie Anwesenheitslisten zu verschiedenen Sofstware´s exportieren. Stellen Sie sicher, dass Sie die richtige Vorlage für den Exportprozess auswählen.

1. Klicken Sie auf Konfiguration der Vorlagen.



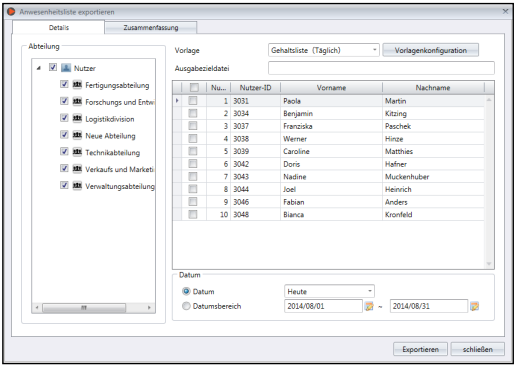
2. Wählen Sie Vorlagen Detail aus, (um Tagesanwesenheitslisten zu exportieren) oder Vorlagen Zusammenfassung (um die Zusammenfassung der Anwesenheitslisten für bestimmte Zeitperiode zu exportieren).
3. Name der Vorlage, z.B. Lohnliste-Projekt X - Details.
4. Klicken Sie auf Bearbeiten.



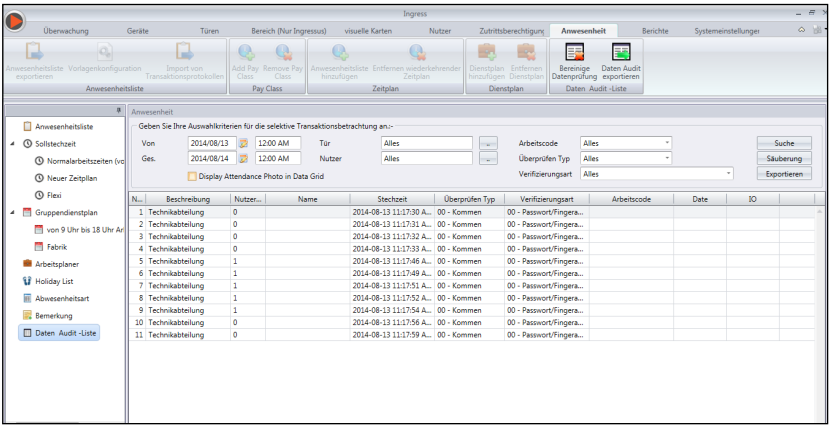
5. Klicken Sie auf Durchsuchen, um den gewünschten Pfad zu ermitteln, um die Ausgabedatei zu speichern. Sie können in XLS oder TXT speichern.
6. Wählen Sie die zu verwendenden Trennzeichen für den Export als TXT-Datei. Ignorieren Sie, wenn Sie in XLS exportieren.
7. Wählen Sie Datenfelder aus dem linken Feld. Klicken Sie doppelt auf das Datenfeld,um es in das rechte Fenster einzufügen.
8. Anordnen der Datenfelder im rechten Fenster, zum exportieren.
9. die Länge des Datenfeldes Anpassen, durch Verändern des Wertes in der Spalte Größe.
10. Klicken auf Speichern, um die Einstellungen zu speichern.

Während des Exportvorgangs:

1. Klicken Sie auf Export-Anwesenheitsplan.
2. Benutzer auswählen einzeln oder Abteilung.
3. Wählen Sie die Vorlage aus.
4. Bestimmen Sie Pfad / Speicherort für die Ausgabedatei.
5. Definieren Sie den Datum des Inkrafttretens der zu expoertierenden Datensätze.
6. Klicken Sie auf Export.



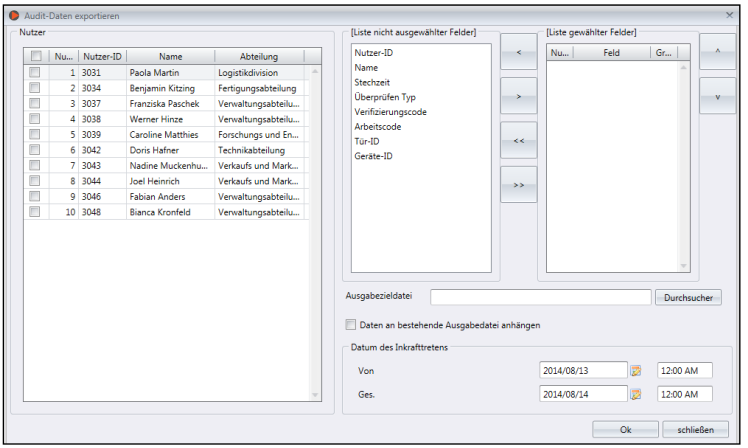
Datenprüfliste



Datenprüfungsliste ist die Datenbank, in der alle Transaktionsprotokolle, die von Geräten heruntergeladen wurden, gespeichert sind. Ingress bietet eine einfache Schnittstelle, die Transaktionsprotokolle zu überprüfen. Alle IN-OUT-Datensätze werden auf dieser Seite veröffentlicht. Sie können die Transaktionsprotokolle, wie folgt anschauen:

- Datumsbereich
- Türen
- Benutzer
- Kurzbezeichnung
- Art der Überprüfung
- Art der Verifizierung

Dies sind Rohdaten, die im XLS, XLSX, TXT-oder CSV-Format exportiert werden können. Die Ausgabedatei kann in eine andere Software zur Weiterverarbeitung oder Auswertung importiert werden.



Stammdaten exportieren:

1. Klicken Sie auf Daten-Audit-List im linken Feld.
2. Klicken Sie auf Export-Data-Audit.
3. Benutzer auswählen Stammdaten, die exportiert werden sollen.
4. Doppelklick, um die Datenfelder auszuwählen, die exportiert werden sollen.
5. Anordnen der Datenfelder, die exportiert werden sollen.
6. Länge einstellen der Datenfelder, durch Verändern ihres Wertes in der Größenspalte.
7. Klicken Sie auf Durchsuchen, um den Pfad zum Speichern der Datei festzulegen.
8. Wählen Sie effective date range, um die Stammdaten zu exportieren.
9. Klicken Sie auf OK, zum Exportieren.

Kapitel 8

Bericht

In diesem Kapitel erfahren Sie, wie man für organisatorische Zwecke, Berichte erzeugen kann.

Ingress bietet Ihnen 8 Typen der am häufigsten verwendeten Berichte. Dazu gehören alle IN-OUT- und Anwesenheitslisten. Sie können Listen von Benutzern, Geräten und Türen erzeugen, die für Ihre zukünftige Organisation sehr nützlich sind.

Sie können die Berichte ausdrucken oder digital in verschiedenen Formaten speichern (PDF, HTML, MHT, RTF, XLS, XLSX, CSV, TXT, XPS und JPEG). Sie können E-Mails mit den digitalen Berichten an andere Personen versenden, die diese benötigen.

Berichten und deren Anwendung

Geräte

Geräteliste: Dieser Bericht zeichnet alle Transaktionsdaten auf, die von jedem Gerät heruntergeladen wurde.

Geräteaktivität: Dieser Bericht beschreibt den Transaktionsdatensatz des Benutzers mittels der Geräte-ID.

Benutzer

Abteilungsliste: Eine Liste mit allen Abteilungen und der zugehörigen Anzahl an Benutzern.

Benutzerliste: Dieser Bericht zeigt ausführliche Informationen der Benutzer.

Bewegungsanalyse der Benutzer: In diesem Bericht werden alle Aktivitäten der Benutzer auf den Geräten aufgeführt.

Türen

Türliste: Dieser Bericht zeigt eine vollständige Liste aller angelegten Türen/Tür-Gruppen mit angeschlossenen Gerät.

Zonen

Gerätetyp mit zugeordneten Zonen.

Zutrittsberechtigung

Liste mit Zutrittsberechtigungen: Dieser Bericht zeigt eine Liste der Türen mit dem zugewiesenen Zutrittsberechtigungen.

Time-Set-Listing: Dieser Bericht zeigt den täglichen Zeitraum für die TimeSet-Konfigurationen.

Urlaubsliste: Dieser Bericht zeigt eine Urlaubsliste, erstellt aus den Urlaubseinstellungen und den zugewiesenen Urlaubszeitzone.

Zutrittskontrolle

Tür-Ereignisbericht: Dieser Bericht ist anwendbar für alle FingerTec-Zugangsgeräte, die mit einem Tür-Sensor verbunden sind. Der Bericht zeigt detaillierte Informationen zur Tür-Ereignissen an.

Transaktionliste: Dieser Bericht zeichnet alle Transaktionsdaten auf, die von jedem Gerät heruntergeladen sind.

Anwesenheit

Zeitplan: Dies ist eine Checkliste mit detaillierten Konfigurationen und Einstellungen des Zeitplans.

Dienstplan: Der Kalender ist eine Arbeitscheckliste für alle Benutzer oder eine bestimmte Arbeitsgruppe.

Bemerkungsliste: Eine Liste aller Arbeits-Codes und ihren Bemerkungen (Namen).

Elektronische Zeitkarte: Der allgemeine Anwesenheitsnachweis der Mitarbeiter setzt sich zusammen aus den detaillierten Zeitaktivitäten eines Mitarbeiters in einem Monat, einschließlich Arbeitszeit, Überstunden und Kurzarbeit. Die Zusammenfassung der Anwesenheit, Verspätung und Urlaub, steht zusätzlich in diesem Bericht zur Verfügung.

Tägliche Anwesenheit: Dieser Bericht beschreibt die tägliche Arbeitszeit, Verspätung, Gesamtarbeitszeit, Überstunden und Minusstunden eines jeden Mitarbeiters.

Wöchentliche Anwesenheit: Dieser Bericht erstellt die wöchentliche Anwesenheit eines Mitarbeiters dar und fasst diese am Ende des Berichtes zusammen.

Anwesenheitsliste: Dieser Bericht ist ähnlich der Zusammenfassung der Anwesenheit, Dieser bildet aber keine Arbeitsstunden, Überstunden oder Minusstunden ab. Mit diesem Bericht kann der Arbeitgeber einen Überblick über Verspätungen und vorzeitiges Arbeitsende der Mitarbeiter bekommen.

Korrekturbericht: Dieser Bericht zeigt unregelmäßige Zeitaktivitäten der Mitarbeiter an, z.B. längere Pausen, vorzeitiges Arbeitsende, Verspätungen, usw. Der Administrator kann diese Aktivitäten der betroffenen Mitarbeiter vergleichen und falls erforderlich ändern.

Verspätungsbericht: Dieser Bericht zeigt die Mitarbeiter mit Verspätungen an. Die Gesamtzeit der Verspätung, in Minuten, werden in Rot angezeigt.

Urlaubsliste: Dieser Bericht zeigt den Urlaub der Mitarbeiter an. Auch Einzelheiten zum Urlaub können entnommen werden.

Überstundenliste: Dieser Bericht zeigt die geleisteten Überstunden aller Mitarbeiter an. Er enthält Details zu Überstundenauf- und Abbau. Dieser Bericht dient zur Übersicht aller Überstunden und der Genehmigung zum Abbau dieser.

Anwesenheitszusammenfassung: Dieser Bericht beschreibt die Arbeitszeiten, Verspätungen, Gesamtarbeitszeiten, Überstunden und Minusstunden für jeden Mitarbeiter. Mit diesem Bericht kann die Arbeitsleitung jedes einzelnen Mitarbeiters eingesehen nund Analysiet werden.

Anwesenheitsanalyse: Dieser Bericht ist der Anwesenheitszusammenfassung ähnlich, aber enthält nicht die Arbeitsleistung, Arbeitszeit, Überstunden und Minusstunden. Der Arbeitgeber erhält einen Überblick , wie oft die Mitarbeiter verspätet sind oder die die Arbeit zu früh beenden.

Tagesanalyse: Dieser Bericht beschreibt die tägliche Arbeitszeit, Verspätung, Gesamtarbeitszeit, Überstunden und Minusstunden für Arbeitstage/Ruhetag und eines Urlaubstages jedes Mitarbeiters.

Monatsanalyse: Dieser Bericht beschreibt die monatliche Arbeitszeit, Verspätung, Gesamtarbeitszeit, Überstunden und Minusstunden für Arbeitstage/Ruhetag und eines Urlaubstages jedes Mitarbeiters.

Kontrollbericht

Kontrollbericht: Dieser Bericht zeigt alle Konfigurationen die in der Software entsprechend der Benutzer eingerichtet sind, die die Bearbeitung durchgeführt haben.

Fehlerprotokoll: Dieser Bericht zeigt alle Fehler, die in der Software aufgetreten sind.

Vorschau, Drucken oder speichern von Berichten

1. Wählen Sie Bericht zur Vorschau oder Drucken.
2. Wählen Sie Filteroptionen aus dem linken Bereich.
3. Klicken Sie auf Erzeugen.
4. Bericht Vorschau an der rechten Bereich.
5. Sonstige Aktionen

Berichte drucken - klicken Sie

Speichern Sie in einem anderen Format:

- Klicken Sie
- Wählen Sie das Datei-Format aus.
- Konfigurieren Sie die Ausgabedatei.
- Klicken Sie auf OK, um fortzufahren.

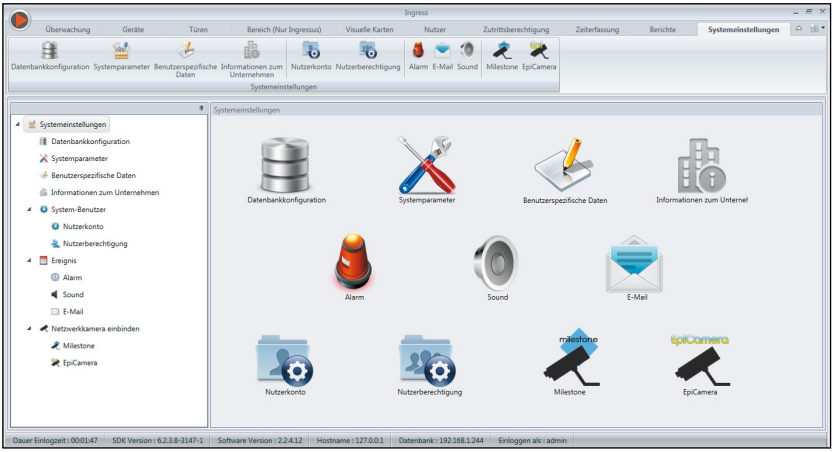
Versenden per E-Mail:

- Klicken Sie
- Wählen Sie das Datei-Format aus.
- Konfigurieren Sie die Ausgabedatei.
- Klicken Sie auf OK, um in eine digitale Datei zu speichern.
- Neue E-Mail wird automatisch von E-Mail-Programm erstellt.
- Setzen Sie die E-Mail-Adressen der Empfänger ein.

Kapitel 9

Ingress Einstellungen

Dieses Kapitel führt Sie durch die Einstellungen der Ingress-Software.

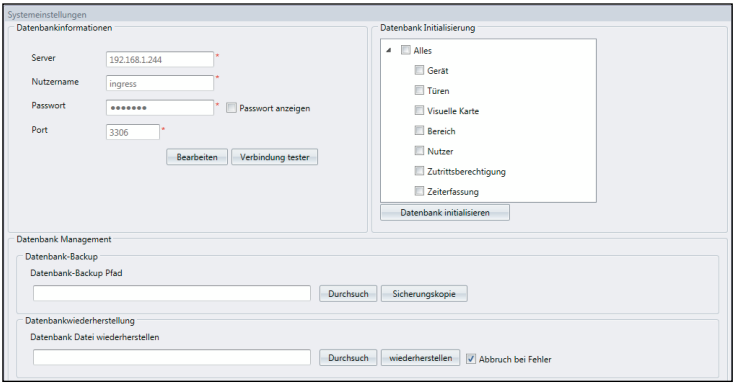


Dieses Kapitel wird Ihnen bei der Konfiguration der Ingress-Software, für Ihre eigenen Bedürfnisse, helfen.

Sie können folgende Einstellungen anpassen:

- Datenbank-Einstellungen: Sie können ein Backup Ihrer MySQL-Datenbank erstellen und jederzeit Wiederherstellen.
- Systemparameter-Einstellungen: Diese Seite ermöglicht Ihnen, Datum, Uhrzeit und andere Anzeigeeinstellungen bei Ingress zu konfigurieren.
- Datenfeld-Einstellungen: Sie können zusätzliche Datenfelder für die Benutzerstammdaten hinzufügen.
- Unternehmensinfo: Erfassen Sie die Information Ihres Unternehmens und Ihres lokalen Händlers. Sie können auch ein spezielles Wasserzeichen in jedem Bericht einsetzen, das von Ingress erstellt wird.
- System-Benutzer: Sie können mehrere Benutzerkonten mit verschiedenen Befugnissen erstellen oder löschen, die Ihre Kopie von Ingress verwenden können.
- Ereignis: Sie können die Ereignisarten konfigurieren, die bei Ingress einen Alarm auslösen. Sie können auch den Ton auswählen, um verschiedene Ereignisse zu unterscheiden. Verbinden sie einen SMTP-Mail-Server, um Benachrichtigungen von Ingress an bestimmte Empfänger zu senden. Für Ingress Mobile Benutzer, können Sie auch Push-Benachrichtigungen einrichten.
- Netzwerkkamera-Integration: Bevor Sie eine Netzwerkkamera anschließen können, um Videomaterial zu übertragen, müssen Sie bei Ingress die Anmeldedaten entsprechend konfigurieren.

Datenbankkonfiguration



1. Füllen Sie die Datenbankinformationen aus:

   Server: IP-Adresse unter der die MySQL-Datenbank eingerichtet ist. Standardmäßig wird MySQL mit dem Ingress-Server installiert.

   Benutzername: Benutzername der MySQL-Datenbank.

   Passwort: Anmeldepasswort der MySQL-Datenbank.

   Port: Richten Sie diesen standardmäßig auf 3306 ein. Ändern Sie diesen, wenn Sie einen anderen Netzwerkanschluss verwenden, um mit der MySQL-Datenbank zu kommunizieren.

2. Klicken Sie auf Verbindung testen, um die Verbindung zur MySQL-Datenbank zu testen. Ändern Sie die Einstellungen, die bei (1) genannt worden sind, wenn die Verbindung fehlschlägt.
3. Klicken Sie auf Speichern, um die Einstellungen zu speichern.

Wenn Sie die MySQL-Datenbank initialisieren möchten (alle in der spezifischen Tabelle gespeicherten Daten zu löschen), gehen Sie folgendermaßen vor.

1. Wählen Sie die Daten aus der Spalte Datenbank-Initialisierung aus.
2. Klicken Sie auf Initialisieren Sie Datenbank.

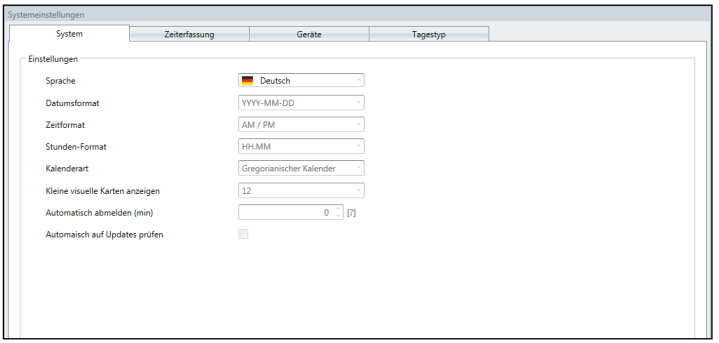
Um die Daten zu Sichern, die bei MySQL-Datenbank gespeichert sind, gehen Sie folgendermaßen vor:

1. Klicken Sie auf Durchsuchen, um den Speicherpfad einzurichten und die Ausgabedatei zu speichern.
2. Klicken Sie auf Backup, um fortzufahren.

Um Daten bei MySQL wiederherzustellen, gehen Sie folgendermaßen vor:

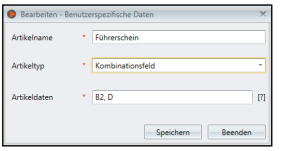
1. Klicken Sie auf Durchsuchen, um die Datei zu suchen, und bei MySQL wiederhergestellt zu werden.
2. Klicken Sie auf Wiederherstellen, um fortzufahren.

Systemparameter-Einstellungen



1. Datum- und Zeitformat: Wählen Sie das Format aus, um Datum, Zeit und Stunde bei Ingress und Berichte anzuzeigen.
2. Anzahl Visuelle Karten: Wählen Sie aus, um 6, 9, 12 visuelle Karten am Bildschirm während der Überwachung anzuzeigen.
3. Auto Abmelden: Richten Sie die maximale Leerlaufzeit ein, bevor das System sich automatisch abmeldet.
4. Server Transaktionsprotokoll: Richten Sie ein Zeitintervall ein, um die Transaktionsprotokolle von Geräten automatisch herunterzuladen. Richten Sie 00:00 ein, um diese Option zu deaktivieren.
5. Entfernen der Transaktionsprotokolle: Aktivieren Sie das Feld, wenn Sie alle Transaktionsprotokolle von Geräten nach dem vollständigen Herunterladen löschen wollen.
6. Geben Sie den täglichen Download-Timer für das System an, um den automatischen Download-Prozess jeden Tag zu aktivieren: Richten Sie bis zu einem Maximum von 2 täglichen Timern ein, die zu einem automatischen Herunterladen der Transaktionsprotokolle von Geräten zu führen.
7. Tägliches Herunterladen, wenn der Computer eingeschaltet ist: Überprüfen Sie die Box, sodass Ingress das tägliche Herunterladen aktiviert, wenn der Server eingeschaltet ist.
8. Der Server erzeugt ein Prüfdatenintervall: Legen Sie das Zeitintervall so an, dass Ingress Rohdaten erzeugt, um die Anwesenheitsliste entsprechend zu aktualisieren. Ignorieren Sie diese, wenn Sie die Anwesenheitsfunktionen bei Ingress verwenden.
9. Verbindungstimeout: Die Geräte trennen sich von Ingress und verbinden sich erneut, wenn das Netzwerk instabil ist. Stellen Sie maximale Wartezeit für Ingress ein, um das Gerät im Offline-Modus einzustellen.
10. Überprüfen Sie synchronisierte Benutzer auf dem Gerät: Aktivieren Sie diese Option und Ingress entfernt immer die Daten aller Mitarbeiter im Gerät oder Ingressus vor dem Hochladen eines neuen Benutzers. Dies dient um sicherzustellen, dass immer eine aktuelle Datenbank auf dem Gerät oder Ingressus verfügbar ist. Deaktivieren Sie diese Option und nur Ingress kann Prozessdaten der Arbeitnehmer in dem Gerät aktualisieren. Ingressus kann dies während des Übertragungsprozesses.

Felddaten-Management

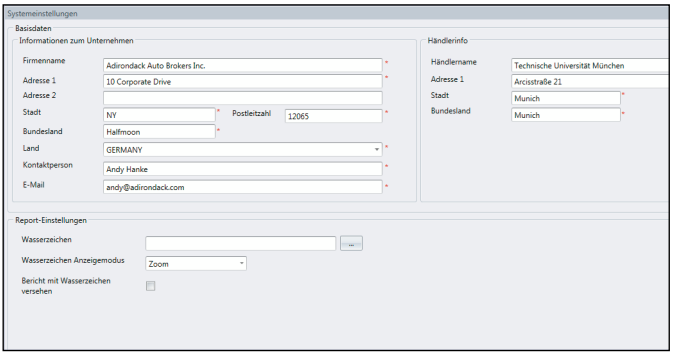


1. Klicken Sie auf Bearbeiten.
2. Klicken Sie auf Hinzufügen, um ein neues Feld hinzuzufügen.
3. Setzen Sie Beschreibung, z.B. Gültiger Führerschein, ein.
4. Wählen Sie das Datenformat aus.
   Textfeld - Spalte, Freitext
   Combo-Box - scrollen Sie herunter, um die Beschreibung hinzuzufügen (erfordert Artikel-Daten).
   Kontrollkästchen - Box zum Aktivieren und Deaktivieren.
   DateCombo box - Kalender zur Datumsauswahl anzeigen.
5. Fügen Sie die Beschreibung in Artikeldaten ein, um für die Combo-Box auszuwählen.
6. Klicken Sie auf Hinzufügen, um Daten in die Liste zu speichern.
7. Klicken Sie auf Speichern, um die Einstellungen zu speichern.

Wiederholen Sie die Schritte, um neue Datenfelder zu erstellen. Alle neu angelegten Datenfelder werden unter Andere Registerkarte Benutzerhandbuch angezeigt.

Klicken Sie auf Aktualisieren, wenn Sie das Datenfeld bearbeiten wollen oder Entfernen um es aus der Liste zu löschen.

Unternehmensinformationen



1. Fügen Sie Ihre Unternehmensinformationen im linken Feld ein.
2. Fügen Sie die Kontaktinformationen von Ihrem lokalen Händler im das rechte Fenster ein.

Folgen Sie den folgenden Schritten, um das Wasserzeichen zu Ihren Berichten einzufügen:

1. Klicken Sie auf ..., um eine Bilddatei (im JPEG-Format) zu wählen.
2. Wählen Sie den Anzeige-Modus aus:

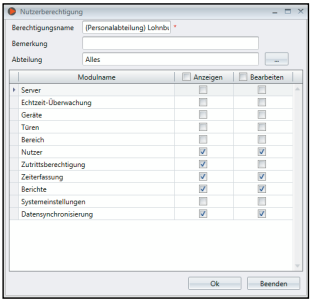
   Zentriert - Wasserzeichen-Darstellung in der Mitte der Seite

   Strecken - Wasserzeichen strecken, um die ganze Seite zu bedecken

   Zoom - Wasserzeichen größer darstellen
3. Aktivieren blenden Sie Wasserzeichen im Bericht ein, um das Wasserzeichen in Berichten zu aktivieren.

Systembenutzer

Benutzerrollen erstellen



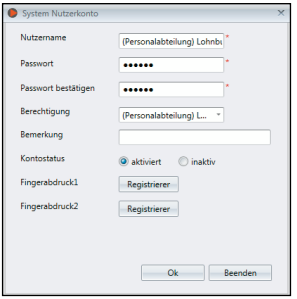
Sie müssen die Benutzerrollen erstellen, um Daten in Ingress bearbeiten oder ansehen zu können. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie auf Benutzerrollen unter Systembenutzer.
2. Klicken Sie auf Rolle hinzufügen.
3. Name die Rolle, z.B. Systembetreiber.
4. Wählen Sie Module aus, um die Ansicht unter der Spalte anzeigen zu ermöglichen.
5. Wählen Sie Module aus, um die Bearbeitung unter der Bearbeiten Spalte zu ermöglichen.
6. Klicken Sie auf OK, um die Einstellungen zu speichern.

Wiederholen Sie die Schritte, um neue Benutzerrollen zu erstellen.

Sie können die bestehenden Rollen aktualisieren, indem Sie diese aus der Liste wählen und auf Rolle bearbeiten klicken.
Wählen Sie vorhandene Rollen aus und klicken Sie auf Entfernen Rolle, um diese zu entfernen, wenn sie nicht mehr im Gebrauch ist.

Um ein Login-Konto zu erstellen und die Rolle zuzuweisen



Jetzt können Sie einen neuen Anmeldebenutzernamen und ein neues Passwort für neue Benutzer erstellen, um Ingress zu verwenden. Handeln Sie wie folgt:

1. Klicken Sie auf Benutzerkonto unter Systembenutzer.
2. Klicken Sie auf Konto hinzufügen.
3. Setzen Sie Benutzername und das Passwort ein.
4. Rolle zuweisen (als Voreinstellung unter Benutzerrolle) zu diesem Konto, z.B. Systembetreiber.
5. Überprüfen Sie die Aktivierung, um den Zugriff auf das Benutzer-Konto zu gewähren.
6. Sie können optional, die Fingerabdrücke von diesem Benutzer einlesen. Dieser kann mit einlesen des Fingerabdruckes Ingress für die Benutzung freischalten, anstatt ein Kennwort zu nutzen. Sie müssen den OFIS-Y-Scanner am PC installieren, bevor Sie auf die [Registrieren] schaltfläche klicken. Folgen Sie den Anweisungen auf dem Bildschirm, um Fingerabdrücke vom Benutzer einzulesen.

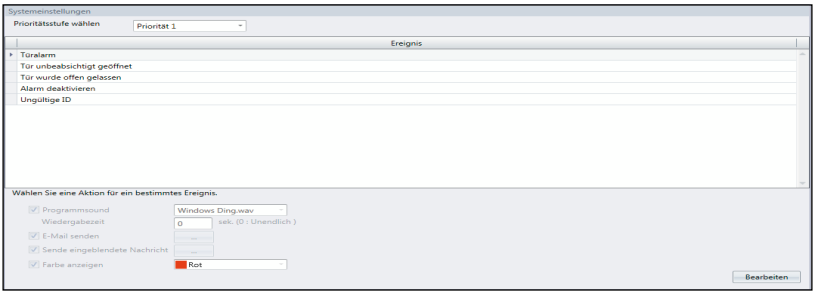
7. Klicken Sie auf OK, um die Einstellungen zu speichern.

Wiederholen Sie die Schritte, um ein neues Login-Konto zu erstellen.

Wählen Sie das Benutzerkonto und drücken Sie Bearbeiten des Kontos, um die Bearbeitung zu beginnen oder drücken Sie Entfernen des Kontos, um das Konto dauerhaft zu löschen.

Ereignis

Benachrichtigungen per Alarm und E-Mail konfigurieren



1. Wählen Sie Alarm unter [Ereignis] aus.
2. Wählen Sie Priorität 1 der Prioritätsstufen aus.

   Sie können für die Ereignisse verschiedene Prioritätsstufen definieren. Es gibt insgesamt 5 Prioritätsstufen, die zur Verwendung bereit stehen. Sie können Stufe 1 als die höchste Stufe und die Stufe 5 als die niedrigste Stufe behandeln, oder umgekehrt.

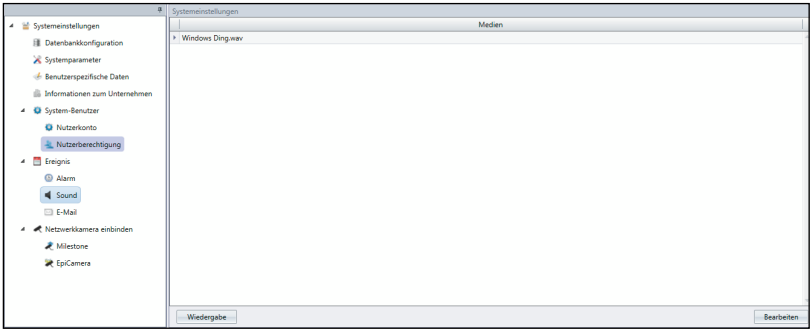
   - Klicken Sie auf Hinzufügen.
   - Wählen Sie Ingressus oder Standalone-Geräte aus.
   - Wählen Sie die Ereignisse aus, um sie der Prioritätsstufe zuzuweisen.
   - Klicken Sie auf OK, um zu speichern.
3. Prüfen Sie Programm-Ton, um ein Alarmton vom PC zu ermöglichen.
   - Wählen Sie Ton abspielen aus, um einen Alarm auszulösen
   - Definieren Sie Dauer der Warnton
4. Wählen Sie E-Mail Senden, um die E-Mail-Benachrichtigungsfunktion zu aktivieren.

   Erstellen Sie eine E-Mail-Vorlage, die als Benachichtigung versendet wird.
5. Wählen Sie Push-Benachrichtigung Senden, um Push-Benachrichtigung an bestimmte Benutzer mit Ingress-Mobile-Anwendungen (*iOS oder Android*) zu aktivieren.

   Wählen Sie die Empfänger der Push-Benachrichtigung aus der Liste aus.
6. Wählen Sie Farbe aus, um die Benachichtigung unter dem Monitoring-Prozess zu markieren.
7. Klicken Sie auf Speichern, um die Einstellungen zu speichern.

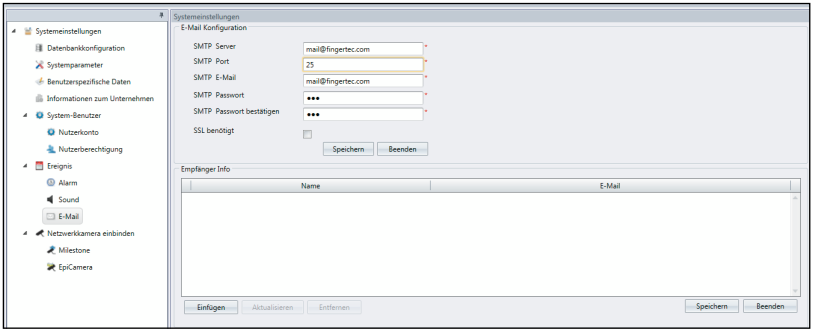
Wiederholen Sie die Schritte, wenn Sie den Alarm zur Priorität 2 bis 5 erstellen wollen.

Alarmsignale und Farbe konfigurieren



1. Klicken Sie auf Ton unter Ereignis.
2. Klicken Sie auf Bearbeiten.
3. Klicken Sie auf Hinzufügen.
4. Wählen Sie eine Sounddatei die zu den Benachichtigungen hinzugefügt werden soll.
5. Klicken Sie auf OK, um die Einstellungen zu speichern.

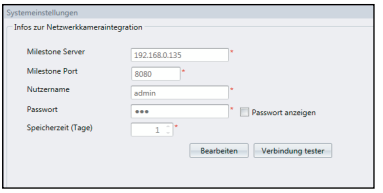
E-Mail-Benachrichtigungen konfigurieren



1. Klicken Sie auf Bearbeiten unter E-Mail-Konfiguration.
2. Fügen Sie die Zugangsdaten zu Ihrem SMTP-Mail-Server ein.
3. Klicken Sie auf Speichern, um die Einstellungen zu speichern.
4. Klicken Sie auf Bearbeiten unter Empfänger-Info.
5. Klicken Sie auf Hinzufügen.
6. Fügen Sie E-Mail-Adresse und Name des Benutzers ein.
7. Klicken Sie auf JA, um die Einstellungen zu speichern.

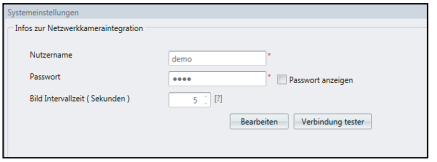
Netzwerk-Kamera-Integration

Milestone-Server



1. Wählen Sie Milestone unter Netzwerk-Kamera -Integration aus.
2. Klicken Sie auf Bearbeiten.
3. setzen Sie die IP und den Port Ihres Milestoneservers ein.
4. Fügen Sie Benutzername und Kennwort ein, um sich beim Meilenstone-Server einzuloggen.
5. Klicken Sie auf Verbindung Prüfen, um sicher zu gehen, dass die Verbindung hergestellt werden kann. Überprüfen Sie Schritt 2 und 3 sollte die Verbindung fehlschlagen.
6. Klicken Sie auf OK, um die Einstellungen zu speichern.

EpiCamera



1. Wählen Sie EpiCamera unter Netzwerk-Kamera-Integration.
2. Klicken Sie aus Bearbeiten.
3. Fügen Sie den Benutzername und das Kennwort Ihres EpiCamerakontos ein.
4. Klicken Sie auf Verbindung Prüfen, um sicher zu gehen, dass die Verbindung hergestellt werden kann. Überprüfen Sie Schritt 3 sollte die Verbindung fehlschlagen.
5. Definieren Sie das Zeitintervall, um die Bilder von der EpiCamera einzusammeln.
6. Klicken Sie auf Ja, um die Einstellungen zu speichern.

FINGERTEC © 2015 Timetec Computing Sdn. Bhd. • Alle Rechte vorbehalten. • 042015